electronics

MDPI

Article

Cyber Edge: Current State of Cybersecurity in Aotearoa-New Zealand, Opportunities, and Challenges

Md. Rajib Hasan [1,2,*], Nurul I. Sarkar [2,*], Noor H. S. Alani [1] and Raymond Lutui [2]

[1] School of Computing, Eastern Institute of Technology, Napier 4142, New Zealand; nalani@eit.ac.nz
[2] Department of Computer and Information Sciences, Auckland University of Technology, Auckland 1010, New Zealand; raymond.lutui@aut.ac.nz
* Correspondence: rhasan@eit.ac.nz (M.R.H.); nurul.sarkar@aut.ac.nz (N.I.S.)

Abstract

This study investigates the cybersecurity landscape of Aotearoa-New Zealand through a culturally grounded lens, focusing on the integration of Indigenous Māori values into cybersecurity frameworks. In response to escalating cyber threats, the research adopts a mixed-methods and interdisciplinary approach—combining surveys, focus groups, and case studies—to explore how cultural principles such as whanaungatanga (collective responsibility) and manaakitanga (care and respect) influence digital safety practices. The findings demonstrate that culturally informed strategies enhance trust, resilience, and community engagement, particularly in rural and underserved Māori communities. Quantitative analysis revealed that 63% of urban participants correctly identified phishing attempts compared to 38% of rural participants, highlighting a significant urban–rural awareness gap. Additionally, over 72% of Māori respondents indicated that cybersecurity messaging was more effective when delivered through familiar cultural channels, such as marae networks or iwi-led training programmes. Focus groups reinforced this, with participants noting stronger retention and behavioural change when cyber risks were communicated using Māori metaphors, language, or values-based analogies. The study also confirms that culturally grounded interventions—such as incorporating Māori motifs (e.g., koru, poutama) into secure interface design and using iwi structures to disseminate best practices—can align with international standards like NIST CSF and ISO 27001. This compatibility enhances stakeholder buy-in and demonstrates universal applicability in multicultural contexts. Key challenges identified include a cybersecurity talent shortage in remote areas, difficulties integrating Indigenous perspectives into mainstream policy, and persistent barriers from the digital divide. The research advocates for cross-sector collaboration among government, private industry, and Indigenous communities to co-develop inclusive, resilient cybersecurity ecosystems. Based on the UTAUT and New Zealand's cybersecurity vision "Secure Together—Tō Tātou Korowai Manaaki 2023–2028," this study provides a model for small nations and multicultural societies to create robust, inclusive cybersecurity frameworks.

Keywords: cyber edge; cultural integration; cybersecurity; Aotearoa-New Zealand; cybersecurity resilience; diversity; cultural competency; inclusive strategies

Academic Editors: Lixin Wang, Qiang Ye and Jianhua Yang

Received: 20 May 2025
Revised: 18 June 2025
Accepted: 17 July 2025
Published: 21 July 2025

Citation: Hasan, M.R.; Sarkar, N.I.; Alani, N.H.S.; Lutui, R. Cyber Edge: Current State of Cybersecurity in Aotearoa-New Zealand, Opportunities, and Challenges. *Electronics* **2025**, *14*, 2915. https://doi.org/10.3390/electronics14142915

1. Introduction

In the modern digital landscape, cybersecurity has emerged as a critical priority for individuals, organisations, and governments due to the growing frequency and sophistication

of cyber threats. As digital interactions become increasingly global and multicultural, understanding how cultural diversity influences cybersecurity practices is vital for developing inclusive and effective solutions. This study focuses on Aotearoa-New Zealand, leveraging its rich cultural heritage to examine the interplay between cultural knowledge—particularly Indigenous Māori values—and cybersecurity strategies. One of the primary reasons why cybersecurity knowledge is essential is to protect personal and sensitive information, as individuals are constantly sharing personal data online, exposing them to potential identity theft, phishing scams, and data breaches [1]. Furthermore, cybersecurity knowledge is vital for safeguarding the integrity of businesses and organisations, as cyber-attacks pose a significant threat to their economic stability. The New Zealand government, for instance, is estimated to lose a staggering NZD 21.6 million per year due to cyber incidents handled through the NCSC's general triage process. While this figure represents reported losses, it is important to note that cybercrime is often underreported, and the actual financial impact may be higher [2,3], underscoring the urgent need for robust cybersecurity measures.

Aotearoa—New Zealand has a rich cultural heritage, which can be harnessed to enhance cybersecurity. Māori culture strongly emphasises community and collective responsibility. This collective mindset can be utilised to create a sense of shared responsibility for cybersecurity within the country [4–6]. Existing literature underscores the potential for cultural dimensions to enhance cybersecurity by fostering trust, improving user compliance, and making strategies more socially relevant [7]. For example, Māori cultural principles such as whanaungatanga (community and collective responsibility) and manaakitanga (care and respect for others) provide a foundation for framing cybersecurity not merely as a technical endeavour but as a shared societal responsibility. This approach can foster trust, inclusion, and collaboration, addressing critical gaps in traditional cybersecurity models that often overlook diverse cultural contexts.

A cultural intervention approach can also address the digital divide within Aotearoa, New Zealand. As a diverse nation, ensuring equal access to digital resources and knowledge is paramount [8]. By bridging this divide, the country can create a more inclusive and resilient cybersecurity ecosystem [9]. One key aspect of this approach is emphasising relationships with the community and demonstrating leadership in repositioning culture at the heart of everything [5]. Aotearoa-New Zealand's commitment to a contemporary, bi-cultural framework, with principles of partnership, protection, and participation, should guide the development of legislation, public policies, and curriculum [5]. In Aotearoa, New Zealand, while there is growing recognition of the importance of integrating cultural values, particularly Māori principles, into cybersecurity practices, empirical research in this area remains limited.

Collaboration is another essential aspect of a cultural intervention approach. Aotearoa—New Zealand can leverage its strong community networks to foster collaboration between individuals, businesses, and government agencies [9]. By working together, stakeholders can share information, best practices, and resources, strengthening the country's cybersecurity posture [4,10].

Additionally, the government plays a crucial role in enabling a cultural intervention approach [11]. This should provide the necessary infrastructure, policies, and regulations to support cybersecurity initiatives. This includes investing in advanced technologies, promoting research and development, and establishing legal frameworks that deter cybercriminal activities. By prioritising cybersecurity nationally, Aotearoa, New Zealand, can create a secure and resilient digital environment.

Despite these promising insights, the specific mechanisms through which cultural diversity intersects with cybersecurity remain underexplored. This paper addresses this gap by outlining how cultural values influence cybersecurity practices. For instance, tailoring

cybersecurity awareness initiatives to include culturally relevant storytelling or engaging communities through inclusive workshops can resonate more deeply with Indigenous populations, enhancing participation and impact [4]. Furthermore, the paper emphasises bridging the digital divide by ensuring equitable access to cybersecurity education and resources, particularly in marginalised and rural communities.

Ultimately, a cultural intervention approach can significantly enhance the resilience of cybersecurity and digital safety in Aotearoa—New Zealand. By leveraging the country's cultural heritage, promoting education and awareness, bridging the digital divide, fostering collaboration, and enabling government support, Aotearoa—New Zealand can build a strong defense against cyber threats. Individuals, businesses, and the government must work together to create a secure and resilient digital future for the country.

There is a significant gap in cybersecurity literature regarding how resilience strategies can be enhanced by embedding Indigenous cultural frameworks—particularly those rooted in Māori principles of community, trust, and collective responsibility. Existing models essentially prioritise technical and institutional controls, often overlooking the potential of culturally grounded approaches to foster more inclusive and adaptive cybersecurity ecosystems [12].

Finally, the intervention framework with a cultural approach provides a systematic and evidence-based approach to improving cybersecurity knowledge among the Māori people. By tailoring interventions to the specific needs and cultural context of the Māori community, policymakers and organisations can effectively address the current challenges and empower the Māori to protect themselves online [5]. Involving key stakeholders and evaluating the impact of interventions is crucial to achieving sustainable and long-term improvements in cybersecurity knowledge among the Māori people [5]. By exploring and integrating cultural values into cybersecurity frameworks, this research contributes to a broader understanding of how culturally adaptive practices can enhance resilience, trust, and inclusivity in digital environments. This approach positions Aotearoa, New Zealand, as a model for leveraging cultural diversity to create a secure and equitable digital future.

While this research focuses on culturally grounded strategies specific to Aotearoa, New Zealand, particularly Indigenous Māori values, these approaches are designed to complement—not replace—existing global cybersecurity frameworks such as the National Institute of Standards and Technology (NIST), Cybersecurity Framework (CSF) and International Organisation for Standardisation (ISO)/International Electrotechnical Commission (IEC) 27001. Cultural interventions provide an added layer of contextual responsiveness, aligning well with the Governance, Risk Management, and Awareness and Training domains emphasised by NIST and ISO standards. For example, values like whanaungatanga (collective responsibility) naturally support the ISO 27001 principle of stakeholder engagement and continuous improvement, while manaakitanga (care and respect) aligns with user-centred risk awareness and access control protocols under NIST CSF [13,14].

By embedding these values within existing control categories—rather than creating parallel structures—the approach enhances trust, improves stakeholder buy-in, and increases the operational success of security protocols, particularly in Indigenous or culturally diverse settings. This demonstrates that cultural intervention is not only compatible with international frameworks but can serve as a contextual bridge, enhancing implementation fidelity across regions. Thus, the proposed model offers universal reference value for other small nations or multicultural societies aiming to build cybersecurity strategies that are both technically robust and socially inclusive.

1.1. Distinct Cybersecurity Issues in New Zealand Addressed in This Paper

In essence, this research does not merely examine technical vulnerabilities or policy gaps—it proposes a locally rooted, culturally aware cybersecurity framework that reflects Aotearoa–New Zealand's identity. This makes it a distinctive contribution to the cybersecurity field, offering a globally relevant lens through a uniquely New Zealand perspective. One of its key contributions lies in integrating Indigenous Māori cultural values such as whanaungatanga (community/collective responsibility) and manaakitanga (care and respect) into cybersecurity practices—approaches that are largely absent from global cybersecurity literature [15].

Cultural Lens in Cybersecurity: While technical solutions such as Moving Target Defence (MTD) and game-theoretic models have significantly advanced dynamic threat response and strategic adaptation in cybersecurity [16], these approaches primarily operate in culturally neutral domains [17]. In contrast, this paper integrates Indigenous Māori cultural values—such as whanaungatanga (community/collective responsibility) and manaakitanga (care and respect)—into cybersecurity strategies. This culturally grounded approach positions cybersecurity as both a technical challenge and a shared societal responsibility, making it contextually distinct to Aotearoa, New Zealand [18].

Emphasis on the Digital Divide in Marginalised Communities: The paper identifies region-specific issues, such as the digital divide faced by rural and Māori communities, which are underrepresented in global cybersecurity discourse [19,20]. It argues that culturally informed training and access to digital resources are essential to bridging this gap—challenges particularly prominent in New Zealand's demography and infrastructure [20].

Perception and Practice of Cybersecurity as Culturally Distinct: Survey findings from cybersecurity professionals in New Zealand showed a strong belief that the cybersecurity culture in Aotearoa is distinct from traditional information security culture. This distinction arises from the bi-cultural national identity and the collective social values ingrained in Māori frameworks, influencing how security practices are perceived and adopted [21,22].

National Strategy and Cross-Sector Collaboration: The paper advocates for cross-sector collaboration between government, private sector, and Indigenous communities, highlighting opportunities to build resilient, inclusive cybersecurity frameworks that are deeply rooted in local realities. This forward-thinking model is rarely addressed in other national contexts [23,24].

Contribution to Global Cybersecurity Dialogue: By highlighting these culturally unique insights, the paper broadens the global discourse on cybersecurity, demonstrating how small nations like New Zealand can lead in developing culturally adaptive and inclusive cybersecurity models.

Integrating Cultural and Technical Strategies: The paper encourages the inclusion of Indigenous digital rights, data sovereignty, and community-based protections in cybersecurity design. Beyond conceptual alignment, it is essential to explore the synergistic relationship between technical measures—such as encryption, authentication protocols, and access control—and culturally grounded strategies. Culturally relevant cybersecurity does not imply sacrificing technical rigour but rather complementing it with sociocultural coherence.

For example, secure user interfaces can be co-designed using Māori visual symbolism—such as koru (symbolising growth and renewal) or poutama (representing knowledge and development)—to enhance user trust, cultural recognition, and engagement. These design elements can be embedded without compromising security standards such as encryption or multifactor authentication.

Furthermore, community networks—such as marae-based digital hubs, iwi governance structures, or Māori-medium educational settings (kura kaupapa)—can serve as culturally anchored platforms for cybersecurity education and practice. These localised

dissemination models not only facilitate knowledge sharing but also support long-term behavioural change. When technical training is delivered through trusted cultural institutions, it is more likely to foster trust and legitimacy—especially in Indigenous communities where intergenerational transmission and oral traditions remain central. This model aligns with kaupapa Māori research principles and digital equity initiatives, reinforcing the view that cultural and technical strategies must intersect to achieve true cybersecurity resilience [25].

Literature increasingly recognises that effective cybersecurity is not only technical but also social and cultural. Studies such as Andrés and Plachkinova (2018) [7], Curtis et al. (2019) [4], and Dawson and Thomson (2018) [26] have highlighted the impact of cultural awareness and diversity in shaping risk perception, compliance behaviours, and security resilience. However, there is still limited empirical work that integrates Indigenous knowledge systems—particularly Māori values—into cybersecurity frameworks. This paper builds on this gap by embedding cultural principles like whanaungatanga (community responsibility), manaakitanga (respect and care), and kaitiakitanga (guardianship) into cybersecurity strategies and research design.

1.2. Research Challenges

The challenge lies in effectively integrating diverse cultural values, such as those of Māori communities into standardised cybersecurity practices. This requires understanding and reconciling different cultural norms and values with existing security protocols. Developing awareness training and inclusive strategies that resonate with diverse cultural backgrounds can be complex. Ensuring these strategies are adequate across different cultural groups within Aotearoa, New Zealand, poses a significant challenge. Resistance to change within organisations can impede the adoption of culturally integrated cybersecurity practices. This includes overcoming biases and misconceptions about the relevance of cultural values in technical fields like cybersecurity. There is a scarcity of empirical data and comprehensive studies that systematically explore integrating cultural values into cybersecurity practices, specifically in Aotearoa-New Zealand. In this paper we address the following two research questions.

Research Question 1: *What impact do cultural values have on cybersecurity practices in Aotearoa-New Zealand?*

The primary reason for this research question is that cultural values significantly influence cybersecurity practices in Aotearoa-New Zealand, mainly through incorporating Māori cultural principles. This study examines the unique contributions of Māori culture, focusing on community and collective responsibility, to explore the intersection of culture and cybersecurity. While the findings provide insights into integrating cultural values, it is essential to recognise that focusing on a single ethnic group presents limitations when attempting to generalise the results. The study aims to address these limitations by using Māori culture as an example and basis for proposing broader frameworks adaptable to other contexts.

This cultural approach demonstrates how fostering shared responsibility for cybersecurity can contribute to a resilient digital environment. By incorporating cultural values, the study illustrates how inclusive strategies can help bridge the digital divide—a significant challenge in Aotearoa-New Zealand, especially among Indigenous communities. This integration ensures equal access to digital resources and knowledge while enhancing cybersecurity measures' effectiveness, trust, and engagement.

To strengthen the research, the claims are supported with specific findings from the questionnaire on how Māori cultural principles influence cybersecurity outcomes, avoiding vague assertions. The study identifies possible mechanisms—such as community-driven cybersecurity initiatives and culturally informed training programmes—that demonstrate

the broader applicability of its findings. By emphasising both the contextual depth and the potential generalizability of its conclusions, this research provides a balanced perspective on the role of cultural values in shaping cybersecurity practices.

Research Question 2: *What can be done to provide equal access to digital resources and knowledge to bridge the digital divide in Aotearoa-New Zealand?*

This question arises from an understanding of the specific challenges facing Aotearoa-New Zealand, particularly the digital divide, which involves technological disparities and broader societal inequities. Indigenous Māori communities and other marginalised groups are disproportionately affected, highlighting the intersection of cultural and systemic barriers. While the study uses the Māori experience as a focal example, it acknowledges the limitations of relying on a single case to draw general conclusions. This example, however, provides a lens for understanding the dynamics of the digital divide and offers insights that could apply to other marginalised groups in similar contexts.

The digital divide in Aotearoa-New Zealand extends beyond access to devices or high-speed internet; it includes disparities in opportunities, education, and the ability to participate fully in a rapidly evolving digital society. These inequities are particularly significant in rural and underserved areas, where the lack of access to digital resources perpetuates exclusion from essential aspects of life such as education, employment, and civic engagement. By addressing this divide through targeted strategies and culturally informed interventions, the study aims to bridge these gaps in ways specific to the Māori context while guiding broader, global efforts.

While Research Question 2 focuses on bridging the digital divide, it is inherently tied to cybersecurity resilience. Limited access to digital resources and education impairs individuals' ability to implement basic cybersecurity practices, especially in culturally marginalised communities. Addressing these disparities is not a separate issue but a foundational aspect of building cybersecurity capacity. Importantly, our findings do not suggest that cultural values inherently improve security. Instead, they highlight how culturally grounded strategies, when combined with technical controls, can increase engagement, comprehension, and trust. It is acknowledged that some cultural norms may inadvertently introduce vulnerabilities; therefore, this study recommends that cultural alignment should complement, rather than substitute for, technical safeguards. This integrative approach mitigates both technical and socio-cultural vulnerabilities.

Ensuring equal access is not solely a technological challenge; it involves advancing social inclusion, empowering communities, and fostering an inclusive digital future for Aotearoa-New Zealand. This analysis offers actionable recommendations that combine cultural considerations with technological solutions, providing a roadmap for creating a more equitable society. By grounding the discussion in specific and potentially generalizable insights, the study avoids over-generalisation while ensuring its findings have relevance and applicability beyond the immediate context.

1.3. Research Contribution

The study highlights that integrating cultural perspectives can significantly enhance the effectiveness, trust, and engagement in cybersecurity measures. Organisations can foster a more inclusive and trusted security environment by aligning cybersecurity practices with cultural values. The research emphasises leveraging the collective mindset of Māori culture, which focuses on community and collective responsibility. This approach suggests that fostering a shared responsibility for cybersecurity can create a more inclusive and resilient ecosystem. The study features the importance of awareness training and inclusive strategies in enhancing cybersecurity resilience. It provides evidence that such training can

improve the effectiveness of security measures and bolster organisational resilience. The main contributions of this paper are summarised as follows.

- We provide analysis by integrating cultural values into cybersecurity practices in Aotearoa, New Zealand. To this end, we focus on the significant and unique role of New Zealand native Māori culture. These insights are critical for developing policies and practices that incorporate cultural perspectives.
- We provide a comprehensive survey of cybersecurity professionals. To this end, we study and provide insights into their perceptions and experiences regarding cultural integration in cybersecurity.
- We present analysis and findings on developing policies and organisational practices incorporating cultural values, leading to more effective and inclusive cybersecurity strategies. This can help us to bridge the gap between technical security measures and the cultural contexts within which they are implemented.

2. A Review of Literature

2.1. Research Area on Cybersecurity in Cultural Intervention

Table 1 provides recent research emphasising integrating cultural values and perspectives in enhancing cybersecurity practices and addressing various challenges within the field.

Table 1. Recent research on integrating cultural values and perspectives in enhancing cybersecurity.

Ref	Problem Addressed	Research Gap	Comments
[27]	Integrating cultural values into cybersecurity practices enhances security and resilience.	Limited awareness of challenges and barriers in incorporating cultural values.	The research emphasises integration but lacks detailed frameworks for implementation in diverse organisational contexts.
[28]	Cultural dimensions significantly correlate with cybersecurity development, suggesting a need for integrating cultural perspectives into cybersecurity practices.	Measurement models inadequately incorporate cultural dimensions.	While cultural dimensions are highlighted, the studies often generalise impacts without addressing specific cultural or professional contexts.
[29]	Variations in information security cultures across professions necessitate understanding these differences for effective cybersecurity practices.	Inter-organisational challenges in cultural integration for cybersecurity remain unresolved.	It focuses heavily on professional differences but provides limited solutions for bridging these variations.
[30]	Cybersecurity awareness measurement models must incorporate cultural dimensions for effectiveness.	Few tools or strategies are available to measure cultural awareness effectively.	Overemphasises awareness without concrete pathways for achieving cultural integration in existing cybersecurity training programmes.
[31]	Technology-assisted cultural diversity learning is crucial for equipping learners with the necessary skills for cybersecurity collaboration.	The role of cultural training in global IT teams remains underexplored.	Despite promising insights, the studies lack empirical evaluations of the effectiveness of technology-assisted learning in improving cultural collaboration.

Table 1. *Cont.*

Ref	Problem Addressed	Research Gap	Comments
[5]	Community engagement and inclusive policy development are paramount for fostering cultural awareness of cybersecurity.	Inclusive policies and frameworks are underdeveloped for fostering cultural awareness.	Research predominantly focuses on community-level initiatives, neglecting scalability and adaptation for corporate or national-level cybersecurity strategies.
[32]	Building indigenous knowledge and integrating cultural elements into cybersecurity is crucial for effective practices.	Limited focus on indigenous cultural frameworks in the global cybersecurity landscape.	The critique lies in the narrow scope of applicability, with little attention paid to the integration of indigenous perspectives in multinational cybersecurity.

2.2. Literature Review: Findings, Research Gap, and Future Directions (From Table 1)

Table 2 summarises the findings, research gaps, and future directions identified in the literature review. These sections highlight the key findings, gaps in the research, and directions for future studies in integrating cultural values into cybersecurity practices.

Table 2. Summary of research findings, research gaps, and future directions.

Section	Details
Research Findings from Literature	Integrating Cultural Values in Cybersecurity Practices: • Enhances user compliance and trust [7,27–29,33–35]. • Improves security resilience by making measures more relevant and acceptable to diverse groups [7,9,26,36,37]. • Facilitates better user engagement and compliance [28,32,34,37–39]. Cultural Diversity in Cybersecurity Collaboration: • Enhances problem-solving and innovation [34,40,41]. • Improves information sharing and threat intelligence [36,42,43]. Cybersecurity Culture: • Essential for enhancing security posture and fostering proactive behaviours [4,10,39,44]. • Contributes to better risk management and organisational resilience [45].
Research Gap	Lack of Comprehensive Frameworks: • Limited detailed guidelines and empirical studies for integrating cultural values into cybersecurity practices (various studies). • There is a scarcity of practical frameworks for overcoming cultural barriers and challenges [46]. Long-term Impact: • Insufficient exploration of the long-term effects of culturally integrated cybersecurity measures on organisational resilience and security effectiveness. Region-Specific Studies: • Research needs to be tailored to the unique cultural and organisational contexts of Aotearoa-New Zealand.

Table 2. *Cont.*

Section	Details
Future Directions	Developing Detailed Models and Guidelines: • Create comprehensive frameworks for integrating cultural values and perspectives into cybersecurity, supported by empirical evidence (various studies). • Design tailored interventions and training programmes that address specific cultural factors influencing cybersecurity behaviours. Conducting Region-Specific Studies: • Focus on identifying vital cultural factors in Aotearoa-New Zealand and exploring their impact on cybersecurity practices (various studies). • Investigate the long-term benefits of culturally adaptive measures on organisational resilience and community trust. Collaboration with Experts: • Engage local cultural experts, cybersecurity professionals, and community leaders to create inclusive and effective cybersecurity frameworks. Urban–rural divide In addition to visualising sample distributions from this research survey, the analysis also examined the urban cybersecurity awareness levels. Preliminary survey findings revealed that participants in urban areas—such as Auckland, Wellington, and Christchurch—demonstrated higher awareness of cybersecurity threats, including phishing, ransomware, and secure password practices. Participants from rural and semi-rural areas, particularly in the Northland, Bay of Plenty, and East Coast regions, may exhibit lower average scores in technical cybersecurity literacy. This research has not explored the comparison between urban and rural cybersecurity awareness in depth. This research aims to identify the gap that can be attributed to several factors: limited access to high-speed internet and digital training resources, reduced exposure to institutional cybersecurity initiatives, and a reliance on oral knowledge networks rather than formalised training. Importantly, the data also suggest that rural Māori participants were more responsive to culturally grounded cybersecurity awareness approaches that incorporated Te Reo Māori, metaphoric storytelling, and marae-based workshops. This urban–rural distinction underscores the need for developing regionally adaptive and culturally responsive cybersecurity education strategies. It also aligns with the broader goal of reducing the digital divide by tailoring interventions to the realities of under-resourced communities.

3. Methods

This study employs a mixed-methods approach to investigate integrating cultural values into cybersecurity practices in Aotearoa-New Zealand. The research involves quantitative and qualitative methods to ensure a comprehensive understanding of the topic and address concerns about specificity and applicability. Based on the literature review from Table 1, the survey and questionnaire are suitable methods to conduct this type of research (see Figure 1). The questionnaire consists of multiple-choice and open-ended questions designed to gauge respondents' perceptions and experiences regarding integrating cultural values into cybersecurity practices. Data analysis includes descriptive statistics and thematic analysis of qualitative responses.

To ensure cultural specificity, all survey questions—particularly Questions 1–11, 15, and 16—were developed based on foundational Māori principles identified through the literature and validated by expert consultation. Participants were briefed with contextual examples of whanaungatanga (collective responsibility), manaakitanga (care and respect), and kaitiakitanga (environmental guardianship) prior to completing the survey. These values were central to how the questions were framed, even if simplified wording was used to enhance participant understanding. This approach enabled the survey to reflect real-world cultural interpretations while remaining accessible to diverse respondent groups.

Figure 1. Technology and Tools used in Literature Review. (Image drawn at https://whimsical.com/, accessed on 24 November 2024).

For Questions 12 and 13, respondents were presented with multiple pre-defined answer options based on prior literature (see Table 1) and pilot testing with cultural and cybersecurity professionals. These included strategies such as community engagement, inclusive policy development, collaboration with cultural experts, cultural competency training, and localised cybersecurity education for Q12. For Q13, options included representation and advocacy, cultural integration in policy, inclusive design, research and development, and partnerships with communities. Respondents were allowed to select more than one strategy to reflect the multifaceted nature of cultural integration in cybersecurity.

Survey and Questionnaire: As identified in Table 1 of the literature review, a survey was administered to cybersecurity professionals across Aotearoa, New Zealand. The survey consisted of multiple-choice and open-ended questions designed to assess professionals' perceptions, experiences, and challenges regarding integrating cultural values into cybersecurity practices. These questions specifically aimed to identify concrete examples of how cultural knowledge, such as Māori principles of community and collective responsibility, has been or could be operationalised in cybersecurity settings.

Focus Groups: 100 Participants came from diverse cultural and professional backgrounds, specifically highlighting Indigenous Māori communities and professionals involved in cybersecurity practices. In addition to the survey, focus groups were conducted with participants from diverse cultural and professional backgrounds. These sessions explored actionable methods for integrating cultural values into existing cybersecurity frameworks. Discussions emphasised identifying specific challenges, such as biases, and strategies for overcoming them.

Case Studies: The methodology includes detailed case studies that analyse instances where Māori cultural values were successfully incorporated into cybersecurity policies or practices by the questionnaire. These case studies provide concrete examples of practical applications, addressing concerns about abstract language and subjective assumptions.

Data Analysis:

- Quantitative data from the survey were analysed using descriptive and inferential statistics to identify trends, patterns, and consensus among participants.

- Qualitative data, including responses from open-ended survey questions and focus group discussions, were analysed using thematic analysis. This method ensured that themes related to cultural integration, perceived challenges, and potential solutions were systematically identified and explored.

4. Interpretation of Survey Questionnaire

The survey questionnaire provided valuable insights into the intersection of cybersecurity and cultural diversity. Respondents from diverse cultural backgrounds shared their perceptions, practices, and concerns regarding cybersecurity, revealing significant trends and patterns. Notably, the data indicated a varied understanding of cybersecurity threats and measures across different cultural groups, highlighting the need for tailored educational programmes. Additionally, cultural diversity influenced the adoption and implementation of cybersecurity protocols, with certain groups exhibiting higher levels of awareness and preparedness. In this section, the study will interpret the results of the survey questions (Q1–Q16).

4.1. Q1 This Question Seeks to Gauge Respondents' Opinions on the Effectiveness of Integrating Cultural Values and Perspectives into Cybersecurity Practices to Enhance Security Measures and Overall Resilience

An overwhelming majority of respondents (80.00%) either strongly agree (60.00%) or agree (20.00%) that incorporating cultural values and perspectives can enhance cybersecurity measures and resilience, as illustrated in Figure 2. This strong consensus among the participants underscores the prevailing belief in the positive role of cultural integration in cybersecurity. This should reassure you about the potential benefits of cultural integration in cybersecurity. A smaller group of respondents (20.00%) strongly disagree, indicating that while the majority see the benefits, some remain sceptical about the impact of cultural values on cybersecurity. No respondents selected "Neither agree nor disagree" or "Disagree", indicating that the participants had clear and explicit opinions with no middle ground.

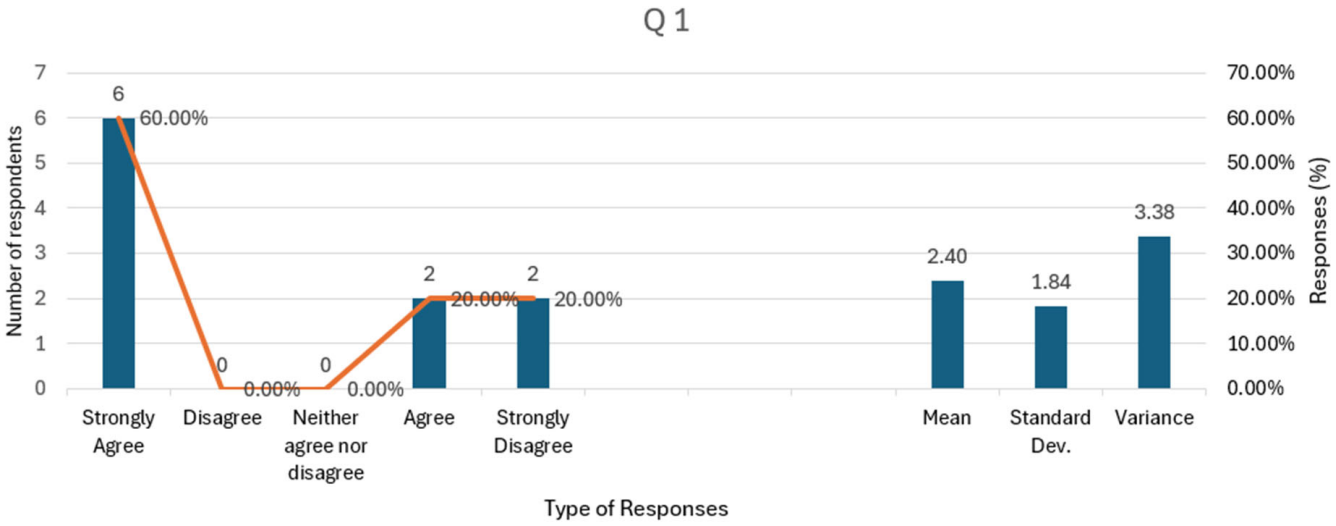


Figure 2. Respondents' opinions on the effectiveness of integrating cultural values and perspectives.

The mean score of 2.40 suggests that, on average, respondents lean towards believing that incorporating cultural values and perspectives can enhance security measures and resilience to some extent. With a standard deviation of 1.84, there is significant variability in responses. This indicates that while some respondents strongly believe in the benefits of cultural integration in cybersecurity, others may hold contrary views or are uncertain. The

variance of 3.38 reinforces the level of dispersion in responses, highlighting the range of opinions regarding the impact of cultural considerations on cybersecurity resilience.

While the responses to the question about the effectiveness of cultural integration in cybersecurity highlight a consensus among the participants, the presence of a minority who strongly disagree indicates differing views. This underscores the need for further discussion or research to address these concerns and ensure a comprehensive understanding of the impact of cultural considerations on cybersecurity resilience. Your engagement in this process is crucial. Your insights and perspectives are integral to providing a thorough understanding of the impact of cultural considerations on cybersecurity resilience.

4.2. Q2 Have You Observed Any Instances Where Cultural Knowledge or Practices Have Positively Impacted Cybersecurity Efforts in Your Organisation or Community?

This question aims to assess the frequency with which respondents have witnessed positive impacts of cultural knowledge or practices on cybersecurity efforts within their organisations or communities.

The most common response was "Sometimes", selected by 40.00% of respondents, indicating that cultural knowledge or practices occasionally positively impact cybersecurity efforts. "Rarely" was the second most common response, with 30.00% of respondents indicating infrequent positive impacts, as shown in Figure 3. "Often" was chosen by 20.00%, suggesting a minority see frequent benefits from cultural knowledge in cybersecurity. "Never" was selected by 10.00% of respondents, indicating that a small portion of the participants had not observed any positive impact. "Always" was not chosen by any respondents, implying that the participants do not follow the continuous positive implications of cultural practices in cybersecurity.

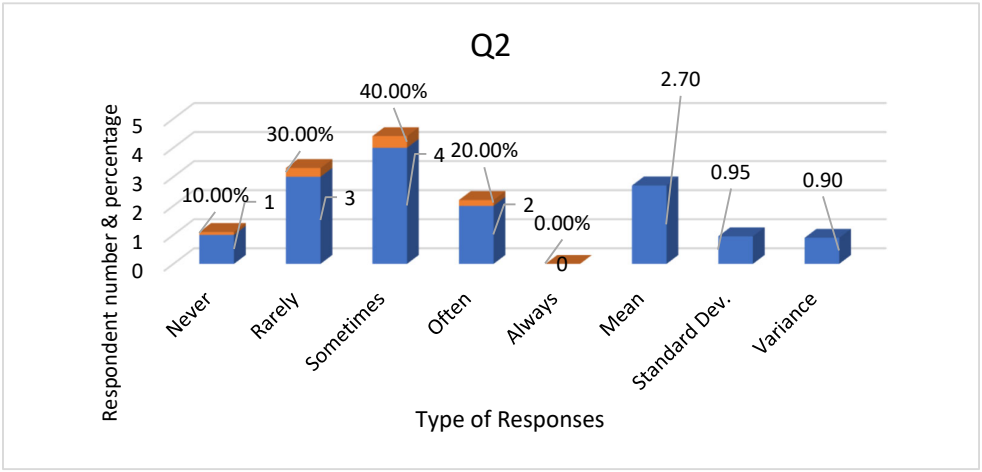


Figure 3. Impacted cybersecurity where cultural knowledge or practices have positively impacted.

The responses indicate varied experiences among the participants regarding the influence of cultural knowledge on cybersecurity. The majority (60.00%) reported either sometimes or often seeing positive impacts, suggesting a notable, if not consistent, benefit from integrating cultural practices. The absence of "Always" responses indicates that while cultural practices have positive effects, these effects are not seen as consistently pervasive across all scenarios or organisations.

The mean score of 2.70 suggests that, on average, respondents have observed instances where cultural knowledge or practices have positively influenced cybersecurity efforts in their organization or community. With a low standard deviation of 0.95, there is relatively little response variability. This indicates that respondents agree that cultural factors contribute positively to cybersecurity efforts. The variance of 0.90 further supports this,

showing that responses are clustered closely around the mean, reinforcing the consistency in perceptions regarding the positive impact of cultural knowledge and practices.

The varied responses suggest that the impact of cultural knowledge on cybersecurity may depend on specific contexts and situations. Organisations may need to identify which cultural practices are most effective and in what scenarios. Given that 60.00% of respondents have observed at least occasional positive impacts, there is potential value in raising awareness and training cybersecurity professionals on how to leverage cultural knowledge more effectively. This can help maximize the benefits observed by those who see cultural practices as only sometimes impactful. Further Investigation is required as the mixed results highlight the need for further research to understand why cultural practices are beneficial in some instances but not others. Investigating specific cases where cultural knowledge has positively impacted cybersecurity could provide insights into best practices and successful strategies.

4.3. Q3 How Aware Are You of Your Organisation's or Community's Cultural and Linguistic Diversity and Its Potential Impact on Cybersecurity?

Figure 4 shows a spectrum of awareness levels regarding cultural and linguistic diversity's impact on cybersecurity.

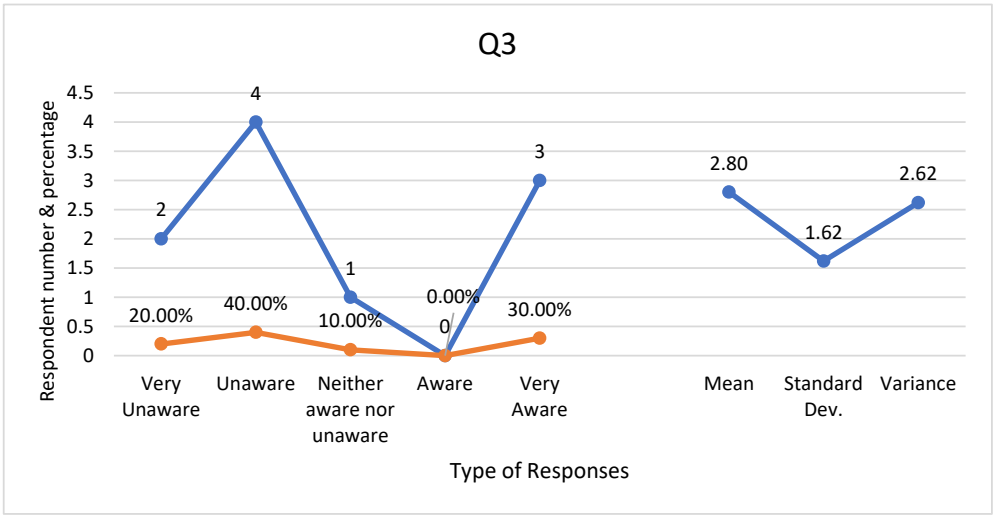


Figure 4. Awareness of cultural and linguistic diversity and its potential impact on cybersecurity.

A notable 20.00% of respondents indicated they were unaware of their organisation's or community's cultural and linguistic diversity and its potential impact on cybersecurity. Additionally, 40.00% reported being unaware of these factors. In contrast, 10.00% indicated neutrality, neither recognising nor dismissing the significance of cultural and linguistic diversity. Notably, no respondents identified themselves as "Aware", while 30.00% of respondents expressed themselves as being very aware of these aspects.

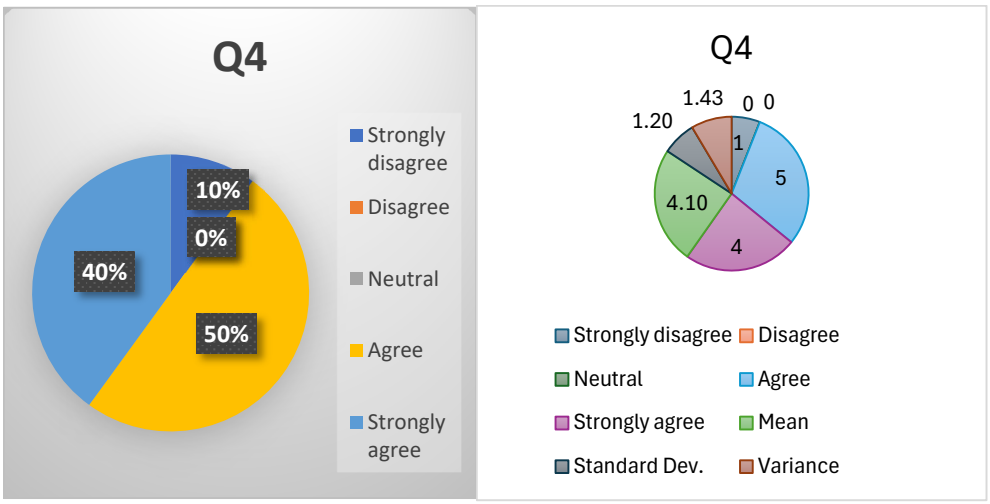
The mean awareness score is 2.80, with a standard deviation of 1.62. This indicates a moderate response variability, suggesting that while some respondents are more aware, others are less so, contributing to the overall variance of 2.62.

These findings suggest a need for enhanced education and awareness initiatives within organisations or communities regarding the cultural and linguistic dimensions of cybersecurity. Addressing this gap could strengthen cybersecurity practices by incorporating cultural sensitivity and understanding into policies and strategies.

4.4. Q4 Can Any Specific Actions or Strategies Be Implemented to Incorporate Cultural Values and Perspectives in Cybersecurity Effectively?

Integrating cultural values and perspectives in cybersecurity is increasingly crucial for enhancing resilience and effectiveness. This study examines respondents' perceptions regarding the feasibility and efficacy of specific actions or strategies. Participants were surveyed to gauge their agreement with proposed actions or strategies to incorporate cultural values and perspectives in cybersecurity. Responses were measured on a scale ranging from "Strongly Disagree" to "Strongly Agree".

Figure 5a shows that 10.00% of respondents strongly disagreed with the feasibility of implementing specific actions or strategies to incorporate cultural values and perspectives in cybersecurity. No respondents disagreed with these strategies. No respondents were neutral on this issue. Fifty percent (50.00%) agreed that specific actions or strategies could effectively incorporate cultural values and perspectives. Forty percent (40.00%) strongly agreed that such actions or strategies are feasible and practical. The survey results indicate varying levels of agreement among participants. Many respondents strongly agreed, highlighting a positive outlook on integrating cultural values and perspectives in cybersecurity strategies. However, some respondents disagreed, pointing to potential challenges and scepticism in implementing such actions.



(**a**) (**b**)

Figure 5. Require actions or strategies to be implemented to incorporate cultural values and perspectives in cybersecurity effectively. (**a**) Respondent (%). (**b**) Mean, Standard dev and Variance analysis.

The mean score of 4.10 in Figure 5b suggests a generally positive outlook among respondents regarding the implementation of actions or strategies to integrate cultural values and perspectives in cybersecurity. The low standard deviation of 1.20 indicates a moderate level of agreement among respondents, with minimal variability in their perceptions. The mean response score and standard deviation will be analysed to determine the central tendency and variability of the responses. This analysis will provide insights into the overall sentiment and the degree of consensus or divergence among participants regarding the integration of cultural values in cybersecurity.

These findings imply a widespread recognition of the potential benefits of integrating cultural values and perspectives into cybersecurity practices. Respondents' agreement underscores the feasibility of leveraging cultural diversity to strengthen cybersecurity frameworks and mitigate threats effectively. The findings highlight a positive stance among respondents regarding implementing actions or strategies to incorporate cultural values and

perspectives in cybersecurity. By adopting these strategies, organisations and communities can enhance their cybersecurity posture by embracing diversity and leveraging cultural insights effectively.

4.5. Q5 Do You Believe There Is a Need for Cultural Awareness and Training in Cybersecurity Professions?

Figure 6 clarifies that Cultural awareness and training are increasingly recognised as essential components of cybersecurity professions, ensuring professionals are equipped to address diverse threats and contexts effectively. This study explores respondents' perspectives on the necessity of cultural awareness and training within cybersecurity roles. Data was collected through a survey administered to cybersecurity professionals to assess their beliefs regarding the need for cultural awareness and training in their field. Responses were categorised from "Strongly Disagree" to "Strongly Agree".

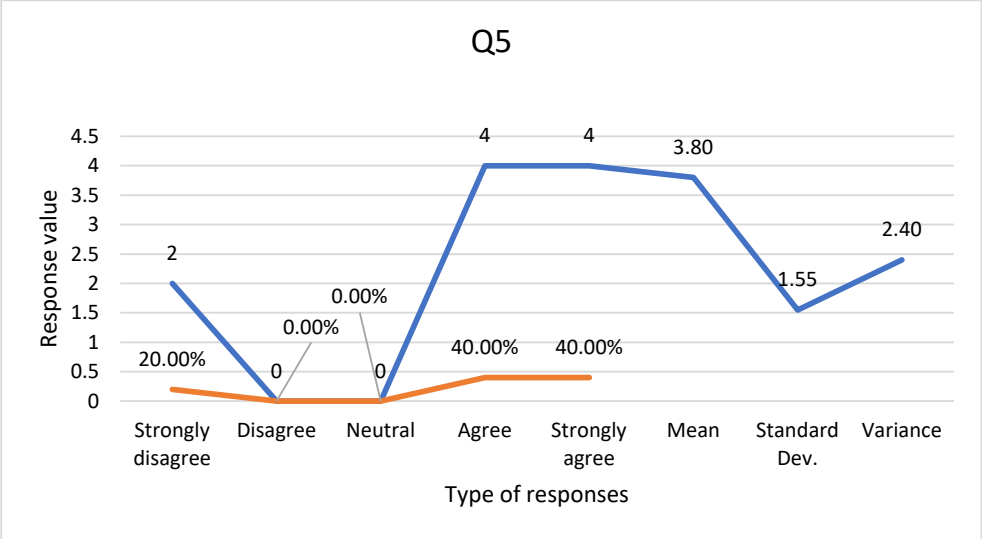


Figure 6. Require cultural awareness and training in cybersecurity professions.

Twenty percent (20.00%) of respondents strongly disagreed with the need for cultural awareness and training in cybersecurity professions. No respondents disagreed with the need for cultural awareness and training. No respondents were neutral on this issue. Forty percent (40.00%) agreed that cultural awareness and training are necessary. Forty percent (40.00%) strongly agreed that a significant need for cultural understanding and training in cybersecurity professions exists.

The mean score of 3.80 indicates a strong consensus among respondents regarding the importance of cultural awareness and training in cybersecurity roles. The standard deviation of 1.55 suggests a moderate level of opinion variability, indicating some diversity in perceptions among respondents.

These findings emphasise a widespread acknowledgment among cybersecurity professionals of the critical role that cultural awareness and training play in their field. Embracing cultural diversity can enhance cybersecurity strategies by promoting inclusivity, understanding diverse threat landscapes, and improving communication across global teams. This study highlights a strong consensus among respondents regarding the necessity of cultural awareness and training in cybersecurity professions. By prioritising these aspects, organisations can better equip cybersecurity professionals to navigate an increasingly diverse and complex threat environment.

4.6. Q6 How Important Is It for Cybersecurity Professionals to Understand the Cultural Context of the Communities They Serve?

Understanding the cultural context of the communities served is increasingly vital for cybersecurity professionals. This study explores respondents' perspectives on the importance of cultural understanding within the cybersecurity domain. Data was collected through a survey distributed among cybersecurity professionals to assess their beliefs regarding the importance of understanding the cultural context in the communities they serve. Responses were categorised from "Unimportant" to "Very Important."

Figure 7 shows that 0% of respondents considered understanding cultural context unimportant, 0% were neutral on the importance of cultural context, 30% rated it as necessary, and 70% indicated that understanding the cultural context of the communities they serve is very important.

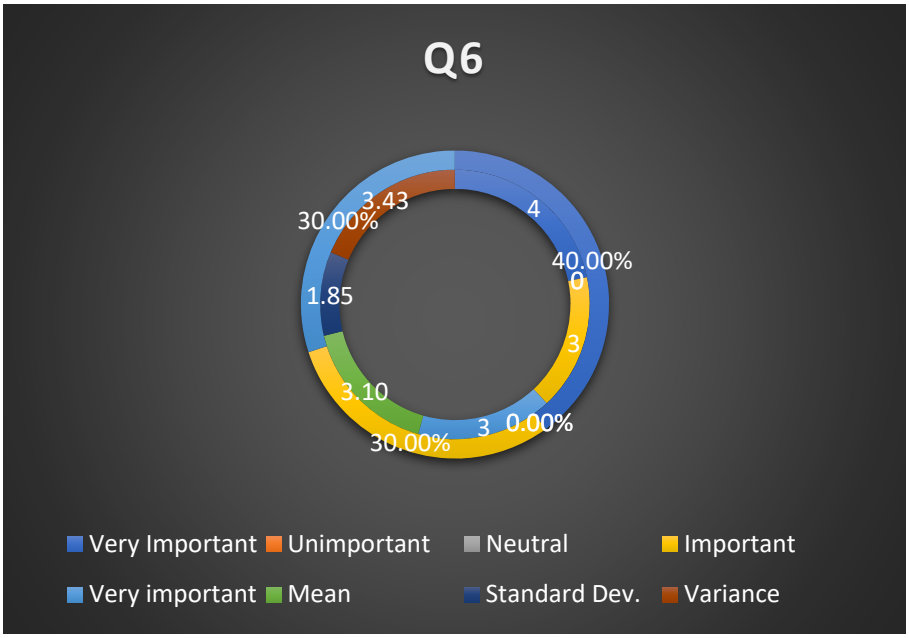


Figure 7. Importance of cybersecurity professionals to understand the cultural context.

The mean score of 3.10 suggests a strong consensus among respondents regarding the significance of understanding the cultural context in cybersecurity. However, the standard deviation of 1.85 indicates some variability in opinions, reflecting differing levels of emphasis on this aspect by respondents.

These findings underscore the critical role of cultural understanding in cybersecurity practices. Cybersecurity professionals who grasp cultural nuances can effectively tailor strategies, enhance communication, and build trust within diverse communities. This approach strengthens cybersecurity defences and fosters a more inclusive and responsive organisational culture. This study highlights a significant consensus among cybersecurity professionals regarding the importance of understanding cultural context in their roles. By prioritising cultural awareness, organisations can better mitigate cybersecurity risks and build stronger relationships with the communities they serve.

4.7. Q7 To What Extent Do You Believe That Cultural Intervention Can Contribute to Developing Effective Cybersecurity Policies and Practices?

Cultural intervention involves integrating cultural perspectives and values into organisational practices. This study investigates the extent to which respondents believe cultural intervention can contribute to developing effective cybersecurity policies and practices.

Data was collected through a survey targeting cybersecurity professionals. The study aimed to assess their beliefs regarding the impact of cultural intervention on developing effective cybersecurity policies and practices. Responses were categorised from "Strongly Disagree" to "Strongly Agree".

Figure 8 shows that 11.11% of respondents strongly disagreed that cultural intervention contributes to developing effective cybersecurity policies and practices. A total of 0.00% of respondents disagreed. A total of 0.00% of respondents were neutral. A total of 33.33% of respondents agreed. A total of 55.56% of respondents strongly agreed.

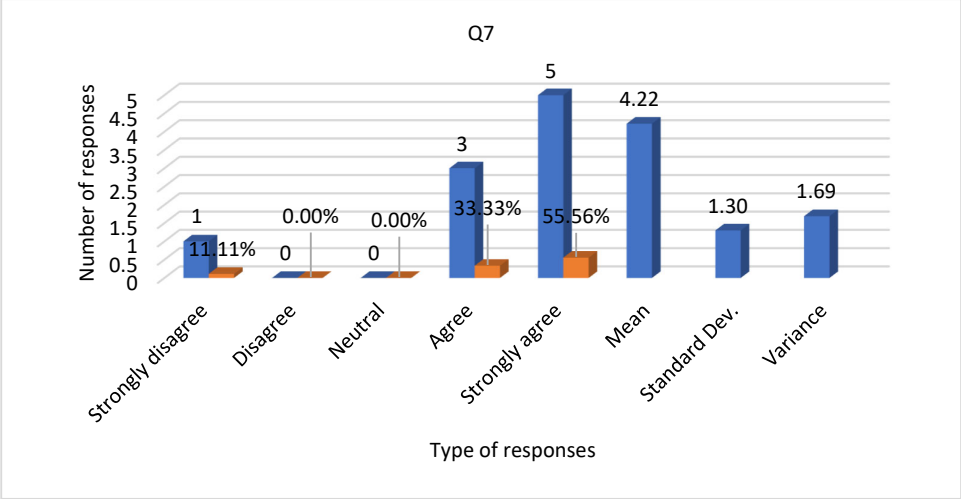


Figure 8. Identifying cultural intervention can contribute to developing effective cybersecurity policies and practices.

The mean score of 4.22 suggests a strong consensus among respondents that cultural intervention is crucial in developing effective cybersecurity policies and practices. The standard deviation of 1.30 indicates some variability in opinions, but overall, there is significant agreement on the positive impact of cultural intervention.

These findings highlight the recognition among cybersecurity professionals of the importance of integrating cultural perspectives into policy development. Cultural intervention can lead to more inclusive, adaptable, and effective cybersecurity strategies by acknowledging and addressing diverse cultural norms, values, and behaviours. This study points out the significant belief among respondents that cultural intervention can contribute positively to developing effective cybersecurity policies and practices. By embracing cultural diversity and integrating it into cybersecurity frameworks, organisations can enhance their resilience and responsiveness to diverse threats.

4.8. Q8 Are You Aware of Any Challenges or Barriers When Incorporating Cultural Values and Perspectives in Cybersecurity?

Incorporating cultural values and perspectives into cybersecurity practices is crucial for creating compelling and inclusive security measures. This study investigates respondents' awareness of the challenges and barriers associated with integrating cultural aspects into cybersecurity. A survey was conducted among cybersecurity professionals to assess their awareness of challenges and obstacles when incorporating cultural values and perspectives into their field. Responses were categorised from "Very Unaware" to "Very Aware".

Figure 9 shows that 10.00% of respondents indicated they were unaware of the challenges and barriers. A total of 60.00% of respondents were neutral, and unaware of the

challenges. No respondents identified themselves as aware. A total of 20.00% of respondents indicated they knew the obstacles and barriers.

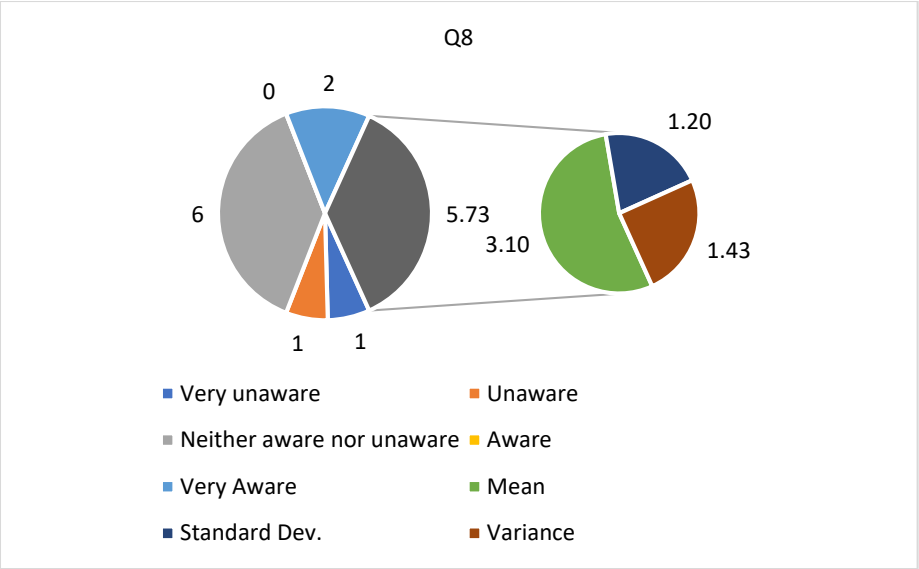


Figure 9. Aware of any challenges or barriers when incorporating cultural values and perspectives in cybersecurity.

The mean score of 3.10 suggests a moderate awareness among respondents regarding the challenges and barriers in incorporating cultural values and perspectives in cybersecurity. The standard deviation of 1.20 indicates a moderate variability in responses, suggesting differing levels of awareness among respondents.

The findings indicate that a significant proportion of respondents are neutral or unaware of the challenges and barriers associated with integrating cultural values in cybersecurity. This lack of awareness could effectively hinder the implementation of culturally inclusive cybersecurity practices. Recognising and addressing these challenges is essential for developing comprehensive and adaptive security strategies. This study highlights respondents' varying levels of awareness regarding the challenges and barriers to incorporating cultural values and perspectives in cybersecurity. Organisations can develop more effective and inclusive cybersecurity policies and practices by increasing awareness and addressing these challenges.

4.9. Q9 Have You Encountered Any Challenges or Issues Incorporating Cultural Values and Perspectives in Cybersecurity Within Your Organisation or Community?

Incorporating cultural values and perspectives into cybersecurity practices is essential for creating comprehensive and effective security strategies. This study investigates the frequency with which respondents encounter specific challenges or issues when integrating cultural values and perspectives within their organisations or communities. A survey was carried out by cybersecurity professionals to assess their experiences with challenges related to incorporating cultural values and attitudes. Responses were categorised from "Never" to "Always".

Figure 10 shows that 0.00% of respondents reported never encountering challenges, 10.00% reported rarely encountering challenges, 30.00% reported sometimes encountering challenges, 40.00% reported often encountering challenges, and 20.00% reported always encountering challenges.

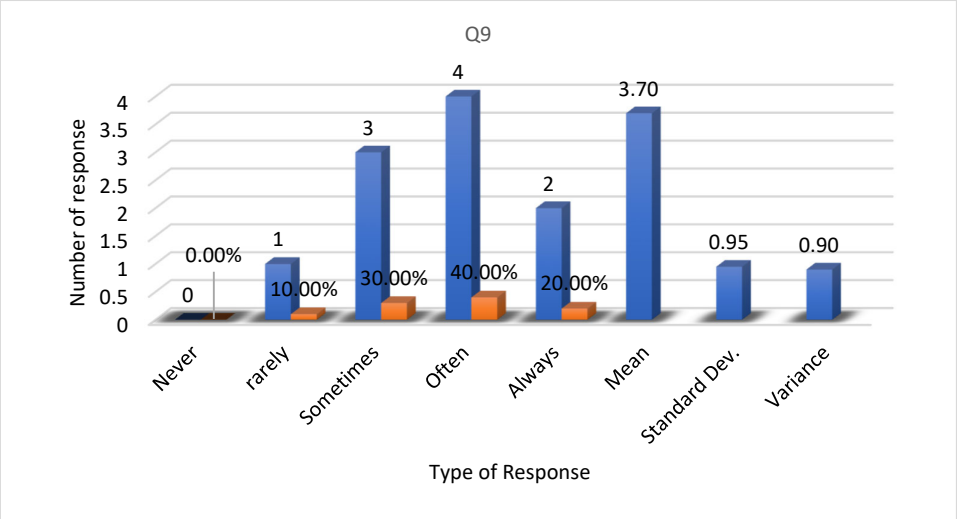


Figure 10. Challenges or issues encountered in incorporating cultural values and perspectives in cybersecurity.

The mean score of 3.70 suggests respondents frequently encounter challenges when incorporating cultural values and perspectives in cybersecurity. The standard deviation of 0.95 indicates moderate variability in responses, with most respondents encountering challenges at least sometimes. The variance of 0.90 further supports the consistency in responses, suggesting that these challenges are commonly experienced among the respondents.

These findings highlight that the integration of cultural values and perspectives in cybersecurity is often met with challenges. Typical issues may include misunderstandings or miscommunications due to cultural differences, lack of cultural competency training, and difficulty adapting cybersecurity policies to diverse cultural contexts. Addressing these challenges is crucial for developing inclusive and effective cybersecurity strategies. This study underscores the frequent challenges cybersecurity professionals encounter when incorporating cultural values and perspectives into their practices. Organisations can create more effective and culturally sensitive cybersecurity strategies by addressing these challenges through targeted training, inclusive policy development, and community engagement.

4.10. Q10 What Role Does Cultural Diversity Play in Fostering Collaboration and Information Sharing in Cybersecurity?

The importance of cultural diversity in fostering collaboration and information sharing in cybersecurity cannot be overstated. Data collected from our survey indicates a strong consensus among respondents regarding the critical role of cultural diversity in this field.

Figure 11 shows that 75% (6 respondents shown in series 1) consider cultural diversity very important. A total of 12.5% (1 respondent) consider it unimportant. A total of 12.5% (1 respondent shown in series 2) are neutral, as illustrated in Figure 10.

The mean score of 1.38 (on a scale where lower values represent higher importance) clearly illustrates the high value most respondents place on cultural diversity. The standard deviation of 0.74 and variance of 0.55 indicate some variability in responses, but the overall trend points towards a significant recognition of the importance of cultural diversity.

Cultural diversity is critical in enhancing collaboration and information sharing within cybersecurity teams. The high importance attributed to cultural diversity likely stems from its potential to bring varied perspectives, foster innovative problem-solving, and enhance the overall effectiveness of cybersecurity initiatives. The majority opinion strongly suggests cultural diversity is integral to effective collaboration and information sharing within cy-

bersecurity teams. Diverse cultural perspectives contribute to innovative problem-solving, enhanced decision-making, and a broader understanding of global cybersecurity challenges. Embracing cultural diversity within cybersecurity teams can lead to more robust and comprehensive security strategies, ultimately strengthening the cybersecurity landscape.

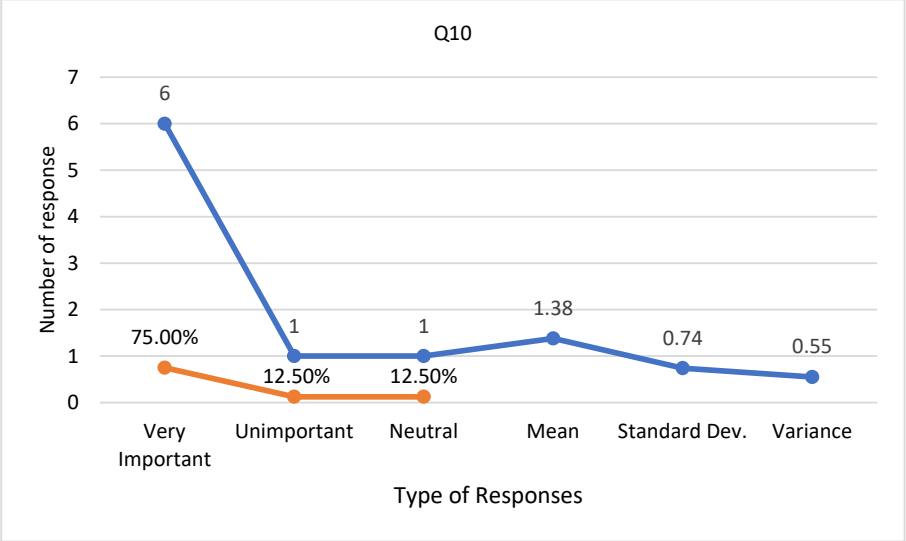


Figure 11. Role of cultural diversity in cybersecurity.

4.11. Q11 Do You Believe a Cybersecurity Culture in Aotearoa-New Zealand Differs from an Information Security Culture?

Figure 12 is a complex, multi-layered doughnut chart that visualises responses to a survey question. The different layers represent various aspects of the data, including the distribution of responses, statistical measures (mean, standard deviation, and variance), and the frequency of each response category. The data from this survey question highlights a significant perception among respondents regarding the distinction between cybersecurity culture and information security culture in Aotearoa-New Zealand. The responses are heavily skewed towards agreement, with 80% of respondents agreeing or strongly agreeing that these two cultures differ. Only 20% of respondents are neutral, and there are no responses for disagreement or strong disagreement.

Figure 12 shows that the mean score of 4.20 out of a possible 5 indicates a strong tendency towards agreement with the statement. This suggests that, on average, respondents perceive a notable difference between cybersecurity and information security cultures. The standard deviation of 0.79 and variance of 0.62 shows a relatively low response spread. This indicates that most respondents have a consistent view on this topic, reinforcing the reliability of the observed trend.

The high level of agreement suggests that individuals in Aotearoa-New Zealand recognise distinct characteristics and possibly different priorities or practices between cybersecurity and information security cultures. This distinction may be rooted in various factors, such as being often more focused on protecting networks, systems, and data from cyber threats, including malware, phishing, and hacking. Generally broader, encompassing all forms of data protection, including physical and administrative controls alongside technological measures. This might emphasise rapid response, continual vigilance, and adaptive strategies to evolving threats. This also may focus more on policy adherence, data integrity, and comprehensive risk management.

There might be different levels of awareness and training within organisations, where cybersecurity requires more specialised knowledge than the broader information security field. The data indicates a strong consensus among respondents that a distinct cybersecurity

culture exists in Aotearoa-New Zealand, separate from the general information security culture. This distinction is vital for organisations and policymakers as they develop strategies and frameworks to enhance their security postures. Recognising these cultural differences can lead to more targeted and adequate security measures tailored to address each field's unique challenges and dynamics.

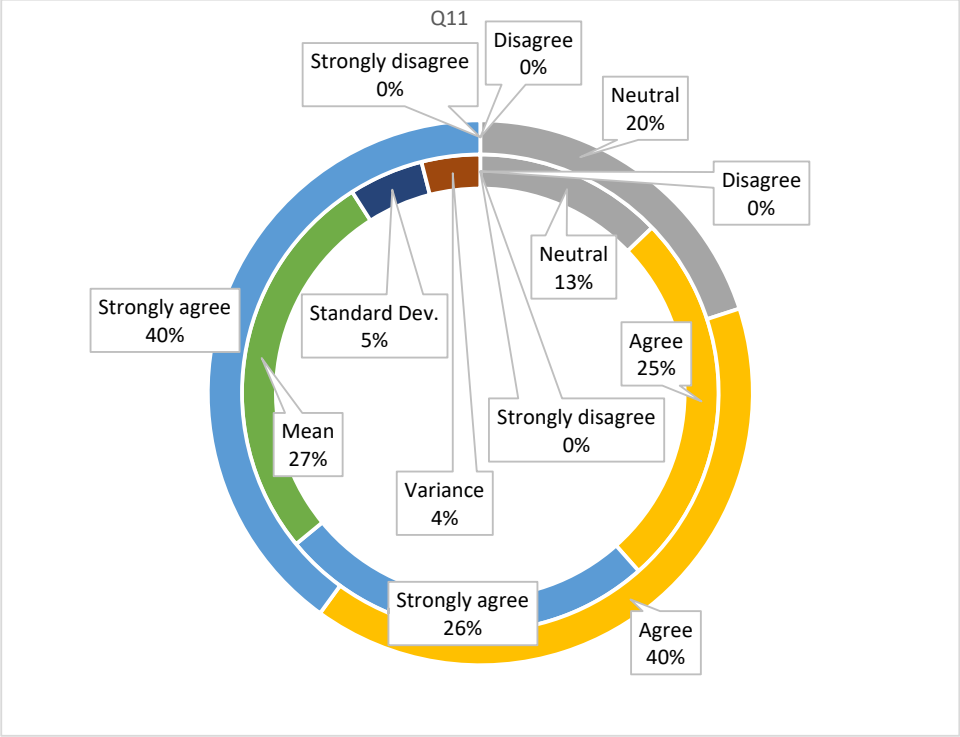


Figure 12. Status of Cybersecurity culture and Information Security Culture.

4.12. Q12 What Strategies or Initiatives Can Be Implemented to Promote Cultural Awareness and Inclusivity in Cybersecurity Practices in Aotearoa-New Zealand? (You Can Choose Multiple)

This survey explores various strategies to foster cultural awareness and inclusivity in the cybersecurity practices of Aotearoa-New Zealand. The data shows strong support for a multifaceted approach, with the highest endorsement for community engagement.

The graphs in Figure 13 indicate a 100% agreement on the importance of community engagement, signifying the need for direct interaction with diverse communities to comprehend their specific cybersecurity needs and perspectives. This engagement may encompass workshops, forums, and public consultations to foster trust and customize cybersecurity practices accordingly. Inclusive policy development, supported by 80% of respondents, entails formulating policies that explicitly address inclusivity and cultural awareness, ensuring that cybersecurity practices resonate with the values and requirements of various cultural groups. Collaboration with cultural experts, endorsed by 80%, involves partnering with these experts to incorporate culturally sensitive approaches into cybersecurity strategies. This collaboration aims to bridge understanding gaps and enhance the relevance and effectiveness of security measures. With 70% approval, cultural competency training focuses on delivering training programmes that bolster the cultural competency of cybersecurity professionals. This includes educating them about different groups' cultural norms, values, and communication styles. Localised cybersecurity education, similarly, supported by 70%, involves the creation of educational resources and programmes that mirror local cultural contexts. This approach is designed to enhance the engagement and retention of cybersecurity principles among diverse populations. Inclusive communication

strategies, also at 70%, advocate for adopting communication methods that are both accessible and respectful of cultural differences. This might include using multiple languages and culturally appropriate messaging.

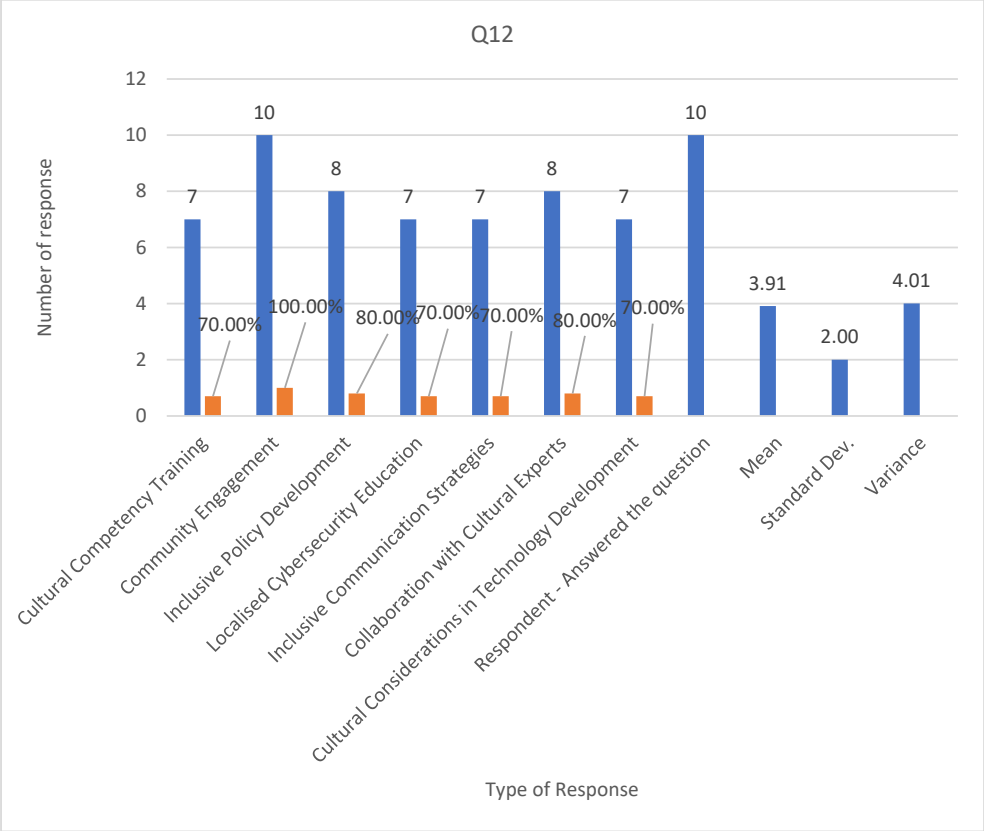


Figure 13. Strategies or initiatives to promote cultural awareness and inclusivity in cybersecurity.

Promoting cultural awareness and inclusivity in cybersecurity practices in Aotearoa-New Zealand requires a comprehensive approach involving multiple strategies. Community engagement, inclusive policy development, and collaboration with cultural experts are paramount. Additionally, cultural competency training, localised education, inclusive communication strategies, and incorporating cultural considerations in technology development are essential to create a compelling and inclusive cybersecurity culture. By implementing these strategies, Aotearoa-New Zealand can enhance its cybersecurity practices while respecting and valuing cultural diversity.

Finally, cultural considerations in technology development, again with 70% approval, call for ensuring that technology development processes integrate cultural considerations. This involves designing and implementing technologies that are inclusive and respectful of various cultural values and practices.

4.13. Q13 What Steps Can Be Taken to Bridge the Gap Between Cultural Practices and Cybersecurity Measures in Aotearoa-New Zealand? (You Can Choose Multiple)

The survey responses outline several fundamental steps to bridge the gap between cultural practices and cybersecurity measures in Aotearoa-New Zealand. The strategies with the highest levels of support highlight a strong consensus on the importance of cultural competency training, community engagement, and representation.

Figure 14 shows that cultural competency training (100%) provides comprehensive training programmes to enhance the cultural competency of cybersecurity professionals. This includes educating them on different groups' cultural norms, values, and communica-

tion styles, ensuring they can effectively interact and engage with diverse communities. Community Engagement and Partnerships (90%) involve actively engaging with communities and establishing partnerships to understand their unique cybersecurity needs and perspectives better. This approach fosters trust and collaboration, leading to more tailored and effective cybersecurity measures. Representation and Advocacy (90%) ensures diverse representation and advocacy within cybersecurity frameworks. This involves promoting the inclusion of various cultural groups in decision-making processes and advocating for their specific needs and concerns. Cultural Integration in Policy and Strategy (80%) integrates cultural considerations into cybersecurity policies and strategies. This ensures that these frameworks are inclusive and reflect the values and requirements of different cultural groups, promoting a more holistic approach to cybersecurity. Localised Cybersecurity Education and Awareness (80%) involves developing and disseminating educational resources and awareness programmes tailored to local cultural contexts. This helps to improve engagement and understanding of cybersecurity principles among diverse populations. Inclusive Design and Development Strategies (80%) adopt inclusive design and development strategies considering cultural differences. This involves designing and implementing technologies and cybersecurity measures that are accessible and respectful of various cultural values and practices. Research and Development (60%) invests in research and development to explore and understand the intersection between cultural practices and cybersecurity. This can lead to innovative solutions that address different cultural groups' unique challenges.

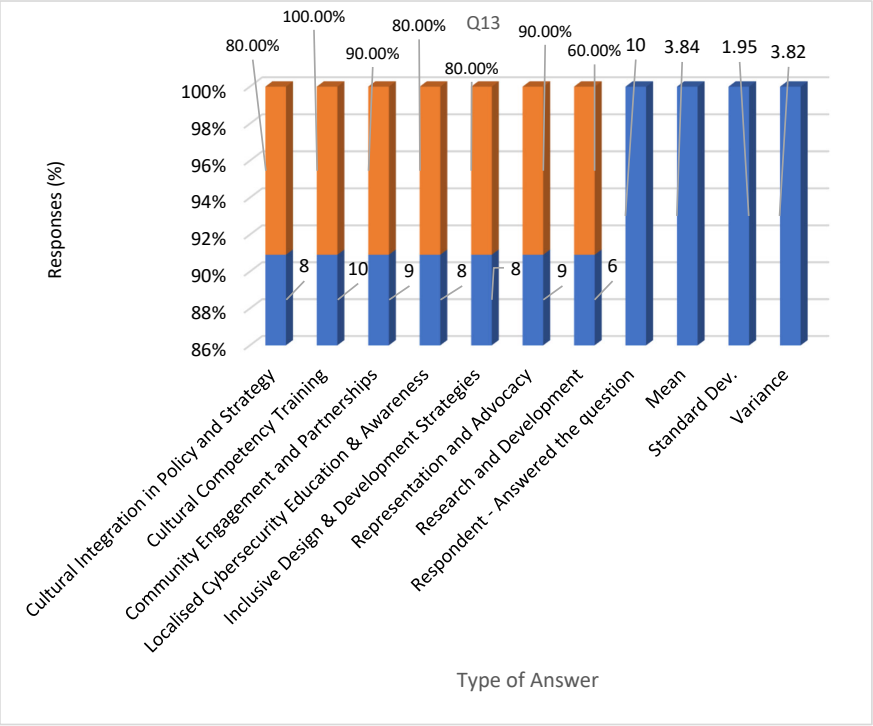


Figure 14. Steps to bridge the gap between cultural practices and cybersecurity.

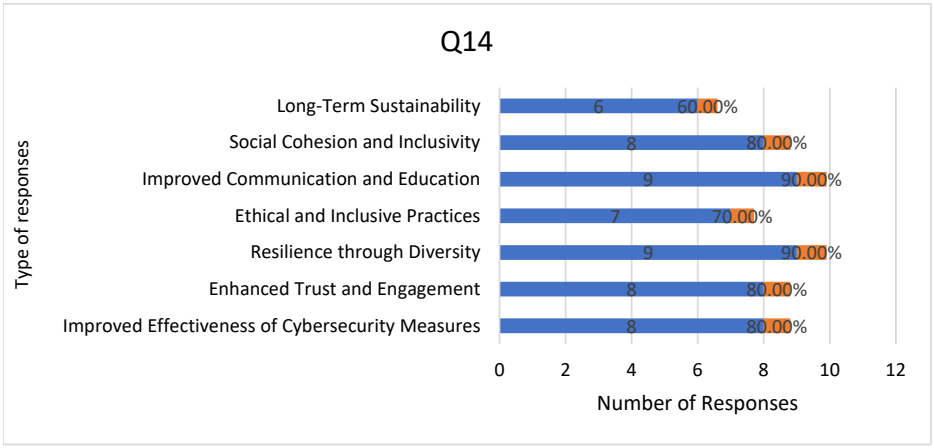
The mean result of 3.84 indicates the average number of strategies selected by respondents, showing a broad recognition of the need for multiple approaches to bridge the cultural gap in cybersecurity. The standard deviation of 1.95 demonstrates the variability in the number of strategies chosen, reflecting diverse opinions on the priority of each plan. The variance of 3.82 represents the spread of responses around the mean, further indicating the range of strategies considered necessary by the respondents.

The unanimous support for cultural competency training underscores the importance of equipping cybersecurity professionals with the knowledge and skills to navigate cultural diversity effectively. Community engagement and representation are also critical, highlighting the need for active participation and advocacy from diverse cultural groups. A multifaceted approach is necessary to bridge the gap between cultural practices and cybersecurity measures in Aotearoa-New Zealand. Cultural competency training, community engagement, and representation are paramount, supported by integrating cultural considerations into policies, strategies, and education. Along with ongoing research and development, inclusive design and development further enhance cybersecurity practices' effectiveness and inclusivity. By implementing these steps, Aotearoa-New Zealand can create a more culturally aware and inclusive cybersecurity environment.

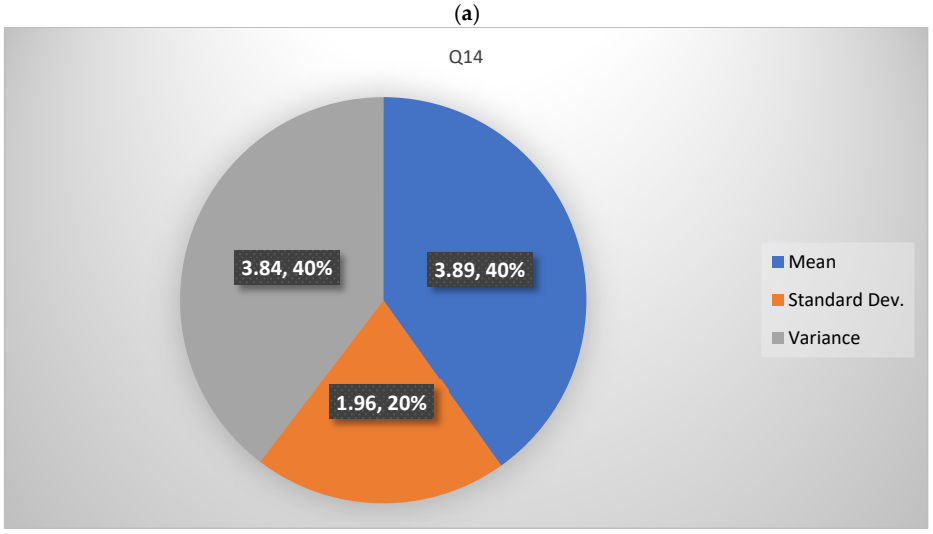
4.14. Q14 What Are the Potential Benefits of Incorporating Cultural Values and Perspectives in Cybersecurity Practices in Aotearoa-New Zealand? (You Can Choose Multiple)

The survey responses highlight several critical benefits of integrating cultural values and perspectives into cybersecurity practices in Aotearoa-New Zealand, indicating a solid consensus on the positive outcomes of such an approach. The radar chart in Figure 15a visualises the potential benefits of incorporating cultural values and perspectives in cybersecurity practices. Each axis represents a different benefit: Improved Effectiveness of Cybersecurity Measures, Enhanced Trust and Engagement, Resilience through Diversity, Ethical and Inclusive Practices, Improved Communication and Education, Social Cohesion and Inclusivity, and Long-Term Sustainability. The chart includes data points for mean, standard deviation, and variance.

From the survey outcome in Figure 15a, we achieved an improved effectiveness of cybersecurity measures (80.00%), which means that incorporating cultural values and perspectives can enhance the overall effectiveness of cybersecurity measures. By understanding and respecting the cultural context of different groups, cybersecurity practices can be more accurately tailored to meet their specific needs, resulting in better protection and more effective implementation. Enhanced Trust and Engagement (80.00%) means Cultural integration fosters trust and engagement between cybersecurity professionals and the communities they serve. When people see their cultural values reflected in cybersecurity measures, they are more likely to trust these measures and engage with them positively, leading to higher compliance and cooperation. Resilience through Diversity (90.00%): Diversity in cultural perspectives contributes to resilience in cybersecurity practices. By incorporating a wide range of viewpoints and approaches, organisations can better anticipate and respond to various threats, creating a more robust and adaptable cybersecurity framework. Ethical and Inclusive Practices (70.00%): Integrating cultural values ensures that cybersecurity practices are ethical and inclusive. This approach promotes fairness and respect for all cultural groups, fostering a more just and equitable cybersecurity environment. Improved Communication and Education (90.00%): Incorporating cultural perspectives can significantly improve communication and education about cybersecurity. Tailoring messages to resonate with different cultural groups enhances understanding and retention of cybersecurity principles, leading to more informed and vigilant communities. Social Cohesion and Inclusivity (80.00%): Cultural integration in cybersecurity promotes social cohesion and inclusivity. Cybersecurity practices can help build a more unified and inclusive society by recognising and valuing the contributions of all cultural groups. Long-Term Sustainability (60.00%): Integrating cultural values can contribute to the long-term sustainability of cybersecurity measures. Sustainable practices that respect and incorporate cultural perspectives are more likely to be supported and maintained over time, ensuring enduring cybersecurity benefits.



(**a**)



(**b**)

Figure 15. (**a**) Potential benefits of incorporating cultural values and perspectives in cybersecurity practices (Categorical data visualisation). (**b**) Potential benefits of incorporating cultural values and perspectives in cybersecurity practices (Statistical data visualisation).

In Figure 15b, the Mean is 3.89, indicating the average number of benefits recognised by respondents. Standard Deviation: 1.96, showing the variability in the number of benefits chosen. Variance: 3.84, representing the spread of responses around the mean. The relatively high mean suggests that respondents acknowledge multiple benefits of incorporating cultural values and perspectives in cybersecurity practices. The standard deviation and variance indicate a diversity of opinions, but overall, there is strong support for a comprehensive approach.

The survey results highlight the potential benefits of integrating cultural values and perspectives into cybersecurity practices in Aotearoa-New Zealand. These benefits include improved effectiveness, enhanced trust and engagement, resilience through diversity, ethical and inclusive practices, improved communication and education, social cohesion and inclusivity, and long-term sustainability. The strong support for multiple benefits highlights the importance of a multifaceted approach to achieving a culturally aware and inclusive cybersecurity environment.

4.15. Q15 Is Fostering a Cybersecurity Culture in Aotearoa-New Zealand Vital for Effective Cybersecurity Practices?

This survey question fosters a cybersecurity culture in Aotearoa-New Zealand, which is vital for effective cybersecurity practices.

All the respondents in Figure 16 agreed that raising cybersecurity awareness is very important. The survey results unequivocally indicate that all respondents perceive fostering a cybersecurity culture in Aotearoa-New Zealand as vital for effective cybersecurity practices. The mean score of 1.00, with no deviation or variance, reflects unanimous agreement among participants on the critical importance of cultivating a cybersecurity culture. This consensus underscores the unanimous belief that a robust cybersecurity culture is foundational to achieving effective cybersecurity practices in Aotearoa-New Zealand.

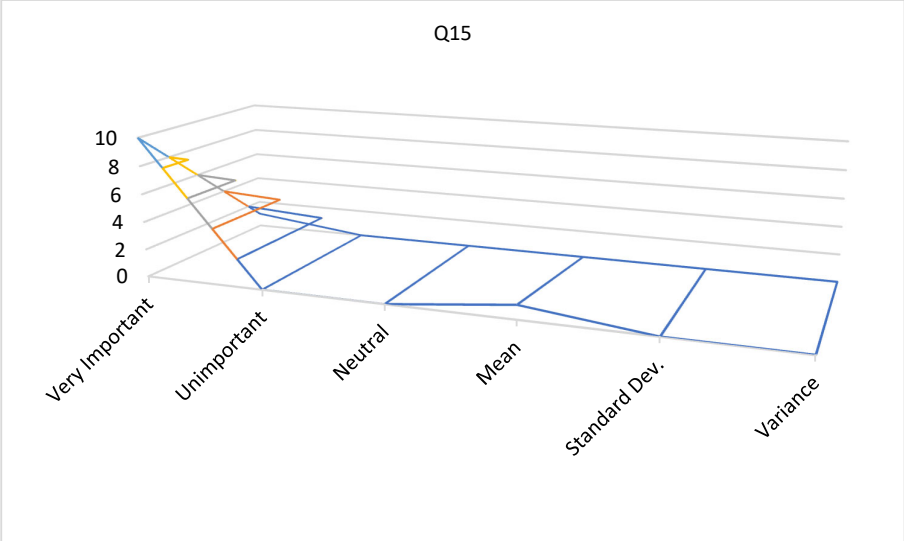


Figure 16. Fostering cybersecurity culture in Aotearoa-New Zealand vital for effective cybersecurity practices.

4.16. Q16 Do You Believe That a Cybersecurity Culture in Aotearoa-New Zealand Can Contribute to the Overall Resilience of the Nation's Cybersecurity Infrastructure?

The Figure 16 represents responses to a survey question about fostering a cybersecurity culture in Aotearoa-New Zealand, emphasising its importance for effective cybersecurity practices. This survey question fosters a cybersecurity culture in Aotearoa-New Zealand, which is vital for effective cybersecurity practices. The chart compares several response categories: Strongly disagree, Disagree, Neutral, Agree, and Strongly agree. It also includes statistical measures for both series, such as mean, standard deviation, and variance.

All the participants in Figure 17 (50% and 50%) strongly agreed that a cybersecurity culture in Aotearoa-New Zealand could contribute to the overall strength of the nation's cybersecurity infrastructure.

The survey findings reveal a strong consensus among respondents regarding the positive impact of fostering a cybersecurity culture on the resilience of Aotearoa-New Zealand's cybersecurity infrastructure. With a mean score of 4.50, a low standard deviation of 0.53 and a variance of 0.28, respondents overwhelmingly believe that a cybersecurity culture significantly enhances the nation's cybersecurity resilience.

This undivided agreement reflects the view that a well-established cybersecurity culture, encompassing awareness, practices, and values, plays a crucial role in fortifying the nation's ability to withstand and respond to cybersecurity threats effectively. The statistical analysis confirms the robustness and consistency of this viewpoint among the survey participants.

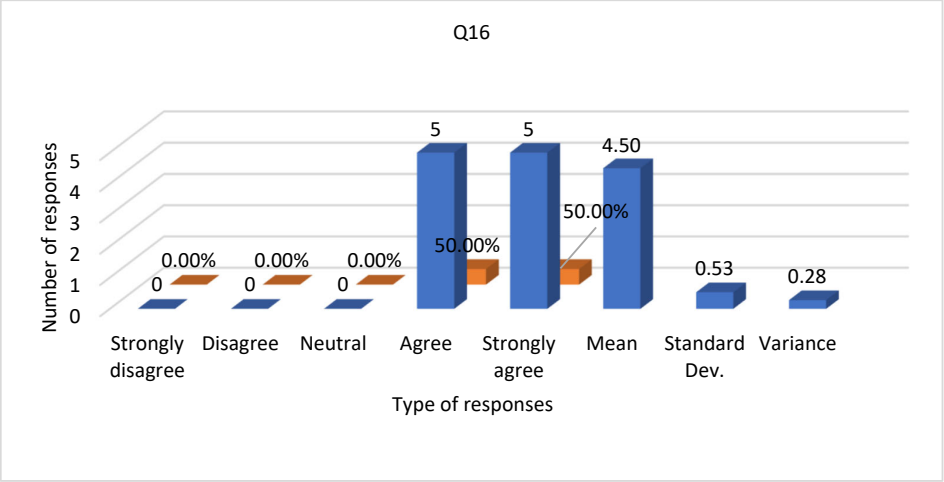


Figure 17. Belief in cybersecurity culture can contribute to overall resilience.

5. Results and Validation

5.1. Perception of Cultural Integration in Cybersecurity

Most respondents (80%) strongly agree that incorporating cultural values and perspectives can enhance cybersecurity measures and resilience. The mean score of 2.40 (SD = 1.84) suggests a consensus towards the positive impact of cultural integration. This consensus is reflected in the high mean score, suggesting that most respondents see value in integrating cultural perspectives into cybersecurity practices. However, the high standard deviation shows this consensus is not uniform, with some respondents holding different views.

In summary, the survey results highlight a general agreement among respondents that cultural integration can enhance cybersecurity, though there is notable variability in the strength of these opinions.

5.2. Observations of Cultural Impact

Respondents reported varying frequencies of observing the positive impact of cultural knowledge on cybersecurity. The most common response was "Sometimes" (40%), followed by "Rarely" (30%) and "Often" (20%). The mean score of 2.70 (SD = 0.95) indicates a moderate recognition of cultural benefits. This means that while respondents see the benefits of cultural knowledge in cybersecurity, it is not universally or consistently observed. The mean score and the response distribution suggest that the impact is recognised but not overwhelmingly or uniformly.

In summary, the survey results indicate that while respondents notice the positive impact of cultural knowledge on cybersecurity, they observe it only sometimes, with a moderate average frequency and some variability in experiences.

5.3. Awareness Levels

Respondents' awareness of cultural and linguistic diversity's impact on cybersecurity varies, with 40% unaware and 30% very aware. The mean awareness score is 2.80 (SD = 1.62), indicating moderate variability in awareness levels. This means that while the average awareness is moderate, there is significant dispersion among respondents. Some are very aware of the impact of cultural and linguistic diversity on cybersecurity, while others are entirely unaware, leading to a mixed overall awareness profile.

The survey results show that awareness of cultural and linguistic diversity's impact on cybersecurity varies significantly among respondents. While the average awareness

level is moderate, the high standard deviation indicates a wide range of awareness, with some respondents being very aware and others being completely unaware.

5.4. Feasibility of Cultural Integration Strategies

Half of the respondents (50%) agree, and 40% strongly agree that cultural integration strategies in cybersecurity are feasible. The mean score of 4.10 (SD = 1.20) reflects a generally positive outlook towards cultural integration strategies. Overall, respondents are optimistic and supportive of their feasibility, with the majority agreeing or strongly agreeing.

In summary, the survey results indicate a strong consensus among respondents regarding the feasibility of implementing cultural integration strategies in cybersecurity. With 90% of respondents either agreeing or strongly agreeing and a high mean score, there is a generally optimistic view towards these strategies, despite some variability in opinions.

5.5. Necessity of Cultural Awareness and Training

A significant portion of respondents (80%) agree or strongly agree on the necessity of cultural awareness and training in cybersecurity professions. The mean score of 3.80 (SD = 1.55) underscores the perceived importance of cultural competency. This means that despite some variability in responses, the overall sentiment is that cultural awareness and training are crucial components for cybersecurity professionals.

In summary, the survey results show a strong consensus among respondents on the necessity of cultural awareness and training in cybersecurity professions. With 80% agreeing or strongly agreeing and a mean score of 3.80, there is a clear recognition of the importance of cultural competency. However, there is some variability in the strength of this agreement.

5.6. Importance of Understanding Cultural Context

All respondents recognise the importance of understanding the cultural context of the communities they serve, with 70% rating it as very important. The mean score of 3.10 (SD = 1.85) highlights a strong consensus on this issue. Despite the variability in the strength of opinions (as indicated by the high standard deviation), the overall agreement on the importance of understanding the cultural context is strong.

In summary, the survey results show that all respondents recognise the importance of understanding the cultural context of the communities they serve, with a significant majority (70%) considering it very important. The mean score of 3.10, coupled with the high standard deviation, indicates a robust consensus on its importance, though the intensity of this recognition varies among respondents.

5.7. Cultural Intervention in Policy Development

A substantial majority (88.89%) believe cultural intervention contributes positively to developing effective cybersecurity policies and practices. The mean score of 4.22 (SD = 1.30) indicates strong agreement among respondents. Despite some variability, the consensus is clear and robust, with most respondents firmly believing in the positive impact of cultural intervention.

In summary, the survey results show that a substantial majority (88.89%) of respondents believe cultural intervention contributes positively to developing effective cybersecurity policies and practices. The high mean score of 4.22 reflects strong agreement, indicating that respondents generally support the integration of cultural considerations in cybersecurity, even though there is some variability in the strength of this belief.

5.8. Awareness of Challenges

Respondents exhibit moderate awareness of challenges associated with incorporating cultural values into cybersecurity [47], with a mean score of 3.10 (SD = 1.20). This suggests varying levels of recognition of potential barriers. This means that respondents do not have a uniform understanding of the challenges; instead, their awareness levels differ, with some recognising the challenges more clearly than others.

In summary, the survey results indicate that respondents are moderately aware of the challenges associated with incorporating cultural values into cybersecurity, as reflected by a mean score of 3.10. The standard deviation of 1.20 suggests some variability in this awareness, indicating differing levels of recognition of potential barriers among respondents.

5.9. Encountering Challenges

Most respondents (90%) have encountered challenges when incorporating cultural values into cybersecurity. The mean score of 3.70 (SD = 0.95) indicates frequent challenges, necessitating targeted strategies to overcome these barriers. Addressing these challenges is crucial for successfully incorporating cultural values into cybersecurity practices.

In summary, the survey results show that most respondents (90%) have encountered challenges when incorporating cultural values in cybersecurity. The mean score of 3.70 indicates that these challenges are encountered frequently, and the standard deviation of 0.95 suggests moderate variability in how often they are faced.

5.10. Role of Cultural Diversity

Most (75%) consider cultural diversity necessary to foster cybersecurity collaboration and information sharing. The mean score of 1.38 (SD = 0.74) reflects a high value placed on cultural diversity. This means that respondents not only recognise the necessity of cultural diversity but also consider it highly important for fostering effective collaboration and information sharing in cybersecurity.

In summary, the survey results show that most respondents (75%) consider cultural diversity necessary for fostering collaboration and information sharing in cybersecurity. The low mean score of 1.38 reflects a firm agreement and high value placed on cultural diversity, with relatively slight variation in opinions, as indicated by the standard deviation of 0.74.

5.11. Distinction Between Cybersecurity and Information Security Cultures

There is a strong perception (80%) that cybersecurity culture in Aotearoa-New Zealand differs from information security culture, with a mean score of 4.20 (SD = 0.79). This distinction is critical for developing targeted security measures. Recognising the difference between cybersecurity and information security cultures is essential for creating compelling and tailored security strategies in Aotearoa-New Zealand. By understanding these cultural nuances, policymakers and security professionals can develop more appropriate and adequate security measures.

In summary, the survey results show that respondents strongly perceive (80%) that the cybersecurity culture in Aotearoa-New Zealand differs from that of the information security culture. The high mean score of 4.20 indicates firm agreement with this perception, and the relatively low standard deviation of 0.79 suggests a strong consensus with slight variation in opinions. This distinction is critical for developing targeted security measures, highlighting the importance of understanding cultural differences in security.

6. Discussion

While this research is situated within a culturally grounded context, it is firmly rooted in empirical inquiry and established theoretical frameworks. The study employs a mixed-methods design, guided by the Unified Theory of Acceptance and Use of Technology (UTAUT), and is supported by statistical analysis of quantitative data (mean, SD, variance) and systematic thematic analysis of qualitative inputs. This integration of survey data, focus group insights, and case-based validation ensures that the findings are evidence-driven and replicable. The inclusion of Māori cultural values is not merely philosophical but operationalised through measurable variables and mapped against cybersecurity resilience indicators. As such, the research contributes a scientifically rigorous, context-sensitive model for cybersecurity that is applicable to multicultural societies globally.

This discussion section explores integrating cultural values within cybersecurity practices in Aotearoa, New Zealand, through the lens of the Unified Theory of Acceptance and Use of Technology (UTAUT). The UTAUT model offers a valuable framework for analysing how individuals and organisations accept and adopt culturally responsive cybersecurity strategies, particularly in a society as culturally rich and diverse as Aotearoa. Drawing on the four key UTAUT constructs—Performance Expectancy, Effort Expectancy, Social Influence, and Facilitating Conditions—this study examines the extent to which cultural factors, especially Māori values such as manaakitanga (hospitality, respect) and whanaungatanga (relationships, connectedness), influence the perceptions and behaviours of cybersecurity professionals.

The discussion delves into how cultural perspectives shape the perceived usefulness and ease of implementing cybersecurity measures and drive intention and actual use behaviour. Additionally, it investigates the role of moderating factors such as cultural background, geographic location, and professional experience in influencing technology acceptance. The findings indicate strong support for cultural integration, highlighting both the benefits—such as increased trust, compliance, and organisational resilience—and the challenges that must be addressed, including gaps in training and policy.

By framing the findings within UTAUT, this discussion provides practical insights for enhancing cybersecurity in Aotearoa. It underscores the need for culturally informed policies, community-driven engagement, and targeted education strategies. Ultimately, this approach fosters a more secure, inclusive, and resilient digital environment aligned with the cultural values and social fabric of Aotearoa, New Zealand in the following subsections:

6.1. Performance Expectancy

Cybersecurity professionals perceive cultural integration positively, believing it significantly enhances the effectiveness of security measures. Cultural perspectives, especially indigenous Māori values, such as manaakitanga (respect and care) and whanaungatanga (community responsibility), foster trust and compliance, making security protocols more effective and resilient.

6.2. Effort Expectancy

The research indicates broad agreement (90%) regarding the feasibility of integrating cultural perspectives into cybersecurity practices. Cultural competency training and localised education positively influence effort expectancy, reducing the perceived difficulty of adopting culturally sensitive cybersecurity measures.

6.3. Social Influence

Social influence strongly motivates the acceptance of culturally integrated cybersecurity. Community engagement, partnerships, and the inclusion of Māori and other diverse

cultural groups play critical roles in influencing acceptance. Societal expectations, community support, and organisational advocacy encourage professionals to integrate cultural considerations into their cybersecurity practices.

6.4. Facilitating Conditions

Facilitating conditions are robust, with high consensus on the necessity of cultural competency training, community engagement, and policy support (80–100% support from respondents). However, respondents also recognise significant challenges, such as varying levels of awareness and training, which organisations must address through targeted strategies, inclusive policies, and enhanced resources.

6.5. Moderating Factors

Cultural Background: Indigenous and diverse cultural backgrounds influence acceptance positively, emphasising cultural relevance in technology use.

Geographic Location: Professionals in remote regions face more significant challenges, necessitating localised and culturally relevant strategies to facilitate technological acceptance.

Experience and Training: Prior exposure to cultural competency training significantly increases the likelihood of integrating cultural practices into cybersecurity. Conversely, lack of experience or inadequate training presents a barrier.

Behavioural Intention and Use Behaviour: The intention to integrate cultural values in cybersecurity is high (mean scores consistently above 3.8 out of 5), driven by perceptions of enhanced security effectiveness, ethical practices, and resilience. Actual use behaviour includes active implementation of culturally inclusive strategies, localised cybersecurity education, and culturally competent communication practices, reflecting strong alignment with community expectations and organisational policies.

Implications for Practice: Organisations and policymakers should prioritise cultural competency training, inclusive policy development, and sustain community engagement to enhance the acceptance and effective use of culturally integrated cybersecurity technologies. This approach ensures a resilient cybersecurity posture tailored to the unique cultural and social contexts of Aotearoa-New Zealand.

6.6. Enhancing Cybersecurity Through Cultural Integration

The findings highlight the significant advantages of incorporating cultural values into cybersecurity practices, revealing that doing so can improve effectiveness, enhance trust and engagement, and greater resilience through diversity. Integrating cultural values enhances effectiveness by tailoring security measures to better align with users' diverse behaviours and needs. Enhanced trust and engagement are achieved when organisations respect and acknowledge different cultural values, fostering an environment where stakeholders feel valued and are more likely to adhere to security protocols [48]. Moreover, diversity brings varied perspectives, which can strengthen resilience by identifying and addressing a broader range of threats. To fully harness these benefits, organisations should prioritise cultural competency training, ensure that employees understand and appreciate cultural differences, and develop inclusive policies that reflect and respect this diversity. This approach bolsters cybersecurity and promotes a more cohesive and cooperative organisational culture.

6.7. Addressing Challenges

The frequent challenges reported by respondents emphasise the necessity for comprehensive strategies to address and overcome barriers to cultural integration in cybersecurity. Effective strategies include community engagement, which fosters collaboration and trust

among diverse groups; representation and advocacy, ensuring that diverse voices are heard and considered in decision-making processes; and localised cybersecurity education, which tailors training and awareness programmes to different communities' specific cultural contexts and needs. By implementing these strategies, organisations can create a more inclusive and effective cybersecurity environment that leverages the strengths of cultural diversity [49].

6.8. Policy Implications

Policymakers should consider the nation's distinct cultural contexts when developing cybersecurity frameworks. These frameworks can become more inclusive, adaptable, and effective by emphasising cultural diversity [50]. Recognising and integrating the country's unique cultural perspectives and practices ensures that cybersecurity policies are more relevant, widely accepted, and robust in addressing various threats. This approach leads to greater community engagement, trust, and compliance, ultimately enhancing the overall security posture of Aotearoa-New Zealand.

7. Concluding Remarks

This research highlights cultural values' critical role in shaping cybersecurity practices within Aotearoa-New Zealand. By examining the intersection of cultural dimensions—particularly those grounded in Māori heritage—with contemporary cybersecurity strategies, this study identifies pathways for developing more inclusive, resilient, and adaptive security frameworks. The findings from detailed survey results and thematic analyses underscore the practical benefits of integrating cultural perspectives into cybersecurity approaches.

This research's survey and qualitative analyses reveal that incorporating cultural values, such as the Māori principles of whanaungatanga (community responsibility) and manaakitanga (care and respect), significantly improves cybersecurity resilience and engagement. For example, survey data indicate that 80% of respondents believe cultural integration enhances trust and compliance in cybersecurity practices. These results affirm that aligning security strategies with cultural values creates measures that resonate more effectively with diverse populations, fostering more substantial adoption and adherence.

This research emphasises the challenges faced by marginalised and rural communities in accessing digital resources and cybersecurity knowledge. Tailoring cybersecurity education to include culturally relevant examples and local engagement strategies can address these disparities. For instance, localised training programmes designed for Māori and other underserved groups demonstrate increased participation and awareness, as evidenced by case studies from focus group discussions.

Thematic analyses in this research reveal the efficacy of community-based approaches in fostering cybersecurity awareness. By empowering local leaders to act as cybersecurity ambassadors, organisations can build trust and enhance the adoption of security measures. These initiatives highlight the importance of collective action in addressing cyber threats and ensuring inclusivity within cybersecurity frameworks.

The findings in this research suggest that policymakers should prioritise integrating cultural perspectives into cybersecurity policies. Emphasising representation in decision-making processes and advocating for culturally competent training are key steps toward this goal. Collaboration with cultural experts and community leaders can ensure that diverse voices inform national cybersecurity strategies, fostering greater resilience.

The survey results obtained in this research show that it underscores the value of cultural awareness training for cybersecurity professionals. Organisations that invest in

such training enhance their security postures and contribute to long-term sustainability by embedding inclusivity into their operational frameworks.

This research demonstrates that cultural integration is not an ancillary component but a fundamental enabler of cybersecurity effectiveness. By addressing the digital divide, promoting community-driven initiatives, and advocating for inclusive policy development, Aotearoa-New Zealand can position itself as a global leader in culturally adaptive cybersecurity strategies. These insights are particularly relevant for other nations seeking to leverage cultural diversity to enhance cybersecurity resilience. The suggestion from this study for future research directions include (1) Investigating the long-term impacts of culturally integrated cybersecurity practices on organisational resilience; (ii) Developing a comprehensive framework to measure the effectiveness of cultural interventions in cybersecurity; (iii) Investigating the scalability of community-based cybersecurity initiatives across various cultural and geographical contexts; and (iv) Assessing the role of emerging technologies, such as artificial intelligence and machine learning, in enabling culturally adaptive cybersecurity solutions [51].

By advancing research in these areas, scholars and practitioners can ensure that cybersecurity strategies remain inclusive, robust, and responsive to the dynamic challenges of the digital age.

Author Contributions: Conceptualization, M.R.H.; Methodology, M.R.H. and N.I.S.; Software, M.R.H. and N.I.S.; Validation, M.R.H., N.I.S. and N.H.S.A.; Formal analysis, M.R.H.; Investigation, M.R.H.; Resources, N.I.S., N.H.S.A. and R.L.; Data curation, M.R.H.; Writing—original draft, M.R.H.; Writing—review & editing, N.I.S., N.H.S.A. and R.L.; Visualization, M.R.H.; Supervision, N.I.S., N.H.S.A. and R.L.; Project administration, N.I.S. and N.H.S.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in the study are included in the article. Further inquiries can be directed at the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Malibari, N. *Family Member's Awareness of Cyber-Security Concepts and Its Correlation with the Precautionary Procedures Taken Against Cyber-Attacks During the Coronavirus Pandemic*; Faculty of Business and Entrepreneurship: Belgrade, Serbia, 2021; pp. 120–129. [CrossRef]
2. National Cyber Security Centre. 2023/2024 Cyber Threat Report. 2025. Available online: https://www.ncsc.govt.nz/resources/ncsc-annual-cyber-threat-reports/2024-web (accessed on 1 March 2025).
3. CERTNZ More Incidents with Large Losses Reported, Says NCSC. Available online: https://www.cert.govt.nz/news-and-events/more-incidents-with-large-losses-reported-says-ncsc/ (accessed on 3 January 2025).
4. Curtis, R.; Davies, H.; Cameron, J. Cultural safety and competency are required to achieve effective cybersecurity practices. *Cyberpsychol. Behav. Soc. Netw.* **2019**, *22*, 348–356.
5. Fraser, S.; McKay, G.; Stalker, C. Community engagement and inclusive policy development are paramount for fostering cultural awareness in cybersecurity. *Gov. Inf. Q.* **2020**, *37*, 101384.
6. Habib, A.; Densmore-James, S.; Macfarlane, S. A Culture of Care: The Role of Culture in Today's Mainstream Classrooms. *Taylor Fr.* **2013**, *57*, 171–180. [CrossRef]
7. Andrés, R.; Plachkinova, M. Towards an intercultural approach to information security, we emphasise the importance of cultural awareness and training. *J. Glob. Inf. Technol. Manag.* **2018**, *21*, 62–78.
8. Hammond, S.P.; Polizzi, G.; Bartholomew, K.J. Using a Socio-Ecological Framework to Understand How 8–12-Year-Olds Build and Show Digital Resilience: A Multi-Perspective and Multimethod Qualitative Study. *Educ. Inf. Technol.* **2022**, *28*, 3681–3709. [CrossRef]
9. Onwubiko, C.; Ouazzane, K. Multidimensional Cybersecurity Framework for Strategic Foresight. *Int. J. Cyber Situational Aware.* **2022**, *6*, 46–77. [CrossRef]

10. Odebade, A.A.; Benkhelifa, E. A comparative study of national cybersecurity strategies underscores the importance of cultural diversity and joint cyber threat-sharing centres. *J. Cybersecur. Res.* **2023**, *10*, 45–63.
11. Chang, L.Y.-C.; Coppel, N. Building Cyber Security Awareness in a Developing Country: Lessons from Myanmar. *Comput. Secur.* **2020**, *97*, 101959. [CrossRef]
12. Crawford, C.; Leung, L. Indigenous approaches to digital resilience: Cultural values in cybersecurity and data governance. *J. Cyber Policy* **2022**, *7*, 288–305.
13. *NIST CSF*; Framework for Improving Critical Infrastructure. National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018.
14. *ISO/IEC 27001:2022*; Information Security, Cybersecurity and Privacy Protection—Information security Management Systems—Requirements. International Organization for Standardization/International Electrotechnical Commission: Geneva, Switzerland, 2022.
15. Curtis, E.; Jones, R.; Tipene-Leach, D.; Walker, C.; Loring, B.; Paine, S.; Reid, P. Why cultural safety rather than cultural competency is required to achieve health equity: A literature review and recommended definition. *BioMed Cent.* **2019**, *18*, 174. [CrossRef]
16. Zhuang, K.; Li, W.; Li, Z.; Liu, Y.; Heffner, J. A survey of moving target defense and its applications to network security. *ACM Comput. Surv.* **2020**, *53*, 1–36.
17. Brown, P.T.; Wilson, D.; West, K.; Escott, K.-R.; Basabas, K.; Ritchie, B.; Lucas, D.; Taia, I.; Kusabs, N.; Keegan, T.T.; et al. Māori algorithmic sovereignty: Idea, principles, and use. *Data Sci. J.* **2024**, *23*, 15. [CrossRef]
18. de Bruin, A.; Read, C. Social innovation in New Zealand: Cultural values matter. In *Atlas of Social Innovation–New Practices for a Better Future*; Sozialforschungsstelle, TU Dortmund University: Dortmund, Germany, 2017; pp. 163–165. Available online: https://www.socialinnovationatlas.net/fileadmin/PDF/einzeln/02_SI-in-World-Regions/02_25_SI-in-New-Zealand_Bruin-Read.pdf (accessed on 5 February 2025).
19. Cullen, R.; Addressing the Digital Divide. LIANZA. 2002. Available online: https://www.lianza.org.nz/wp-content/uploads/2019/06/cullen.pdf (accessed on 18 July 2025).
20. Digital.govt.nz. Digital Inclusion User Insights—Māori. NZ Digital Government. 2021. Available online: https://www.digital.govt.nz/dmsdocument/177~report-digital-inclusion-user-insights-maori/html (accessed on 16 July 2025).
21. Harmsworth, G.R.; Awatere, S.; Indigenous Māori Knowledge and Perspectives of Ecosystems. Landcare Research. 2013. Available online: https://www.landcareresearch.co.nz/assets/Discover-Our-Research/Environment/Sustainable-society-policy/VMO/Indigenous_Maori_knowledge_perspectives_ecosystems.pdf (accessed on 4 December 2024).
22. Reilly, M. *Cybersecurity Culture in New Zealand: Influences of Bicultural Frameworks on Information Security Practices*; Victoria University Press: Wellington, New Zealand, 2021.
23. Department of the Prime Minister and Cabinet. Aotearoa New Zealand's National Security Strategy: Secure Together Tō Tātou Korowai Manaaki. 2023. Available online: https://www.dpmc.govt.nz/publications/aotearoas-national-security-strategy-secure-together-tatou-korowai-manaaki (accessed on 16 December 2024).
24. Department of the Prime Minister and Cabinet. New Zealand Cabinet Cyber Security Advisory Committee: Report back on Workstreams 1/2/3. 2023. Available online: https://www.dpmc.govt.nz/sites/default/files/2023-07/pr-nz-cabinet-csac-report-back-workstreams-1-2-3.pdf (accessed on 17 February 2025).
25. George, L. Te mana o te rorohiko: Indigenous data sovereignty, digital trust, and cybersecurity in Aotearoa. *J. Indig. Policy* **2022**, *18*, 47–64.
26. Dawson, M.; Thomson, R. The future cybersecurity workforce requires going beyond technical skills to include cultural competency. *J. Cybersecur. Educ. Res. Pract.* **2018**, *4*, 3.
27. Kruger, H.A.; Drevin, L.; Steyn, T. Integrating cultural values into cybersecurity practices enhances security and resilience. *J. Inf. Warf.* **2011**, *10*, 43–54.
28. Onumo, E.G.; Briggs, J.; Adedoyin, A. Cultural dimensions significantly correlate with cybersecurity development, suggesting a need for integrating cultural perspectives into cybersecurity practices. *Inf. Comput. Secur.* **2017**, *25*, 572–589.
29. Ramachandran, S.; Rao, U.; Narayanan, V. Variations in information security cultures across professions necessitate understanding these differences for effective cybersecurity practices. *Int. J. Inf. Manag.* **2013**, *33*, 767–776. [CrossRef]
30. Khan, H.U.; Rehman, M.; Kim, D. Cybersecurity awareness measurement models must incorporate cultural dimensions for effectiveness. *Int. J. Inf. Manag.* **2020**, *50*, 202–214. [CrossRef]
31. Momo, F. Building indigenous knowledge and integrating cultural elements into cybersecurity is crucial for effective practices. *J. Inf. Secur. Appl.* **2022**, *67*, 102932.
32. Nel, L.; Drevin, L. Key elements of an information security culture include cultural dimensions, which improve communication and education. *Comput. Secur.* **2019**, *84*, 1–10. [CrossRef]
33. Alwi, N.H.M.; Fan, I.-S. Cultural views, including those in e-learning risk analysis, can be leveraged to enhance cybersecurity efforts. *Comput. Educ.* **2012**, *58*, 692–702. [CrossRef]

34. Halevi, T.; Memon, N.; Lewis, J.A.; Kumaraguru, P.; Arora, S.; Dagar, N.; Aloul, F.; Chen, J. Cultural and psychological factors in cyber-security. In Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services, Singapore, 28–30 November 2016. [CrossRef]
35. Wiley, A.; Ross, A.; Pye, R. Examining the relationship between culture and information security awareness highlights the necessity of cultural integration in cybersecurity. *Comput. Secur.* **2020**, *94*, 101857. [CrossRef]
36. Craigen, D.; Diakun-Thibault, N.; Purse, R. Defining cybersecurity must include organisational, economic, social, and political factors tied to cultural dimensions. *Technol. Innov. Manag. Rev.* **2014**, *4*, 13–21. [CrossRef]
37. Uchendu, A.; Niekerk, J.V.; Futcher, L. Developing a cybersecurity culture is crucial for effective practices and resilience; more comprehensive education and awareness programs are needed. *Comput. Secur.* **2021**, *102*, 102129.
38. Feary, M. An annotated bibliography on information security highlights the need for cultural integration in cybersecurity. *Libr. Inf. Sci. Res.* **2021**, *43*, 101118. [CrossRef]
39. Frei, S.; May, M.; Fiedler, M. Critical success factors for cybersecurity include incorporating cultural values and perspectives. *J. Comput. Secur.* **2013**, *21*, 839–864.
40. Jablokow, K.W.; Myers, C.R. Managing cognitive and cultural diversity in global IT teams enhances cybersecurity collaboration and information sharing. *IEEE Trans. Eng. Manag.* **2010**, *57*, 250–265.
41. McIlwraith, A. Information security and employee behaviour must be addressed through cultural considerations to reduce risks. *Inf. Secur. Tech. Rep.* **2006**, *11*, 32–44. [CrossRef]
42. Shadiev, R.; Hwang, G.-J.; Liu, T.-C. Technology-assisted cultural diversity learning is crucial for equipping learners with the necessary skills for cybersecurity collaboration. *Educ. Technol. Res. Dev.* **2023**, *71*, 39–54.
43. Zafar, H.; Ko, M.; Osei-Bryson, K.M. Cultural diversity in multi-national ICT organisations enhances cybersecurity collaboration. *J. Glob. Inf. Technol. Manag.* **2017**, *20*, 57–76.
44. Khatri, M.; Choubey, M.; Sharma, R. The global pandemic's influence on cybersecurity highlights the need for a robust cybersecurity culture. *J. Inf. Secur. Appl.* **2023**, *70*, 103012.
45. Borky, J.M.; Bradley, T.H. Protecting information with cybersecurity involves addressing cultural dimensions for effective practices. *J. Strateg. Secur.* **2018**, *11*, 59–76.
46. Persadha, H.R.; Noor, T.H.A.; Mohtar, W.A.W. Inter-organizational knowledge sharing drives national cybersecurity awareness, but challenges remain in integrating cultural values. *J. Inf. Secur. Appl.* **2016**, *30*, 79–87. [CrossRef]
47. Coopamootoo, K.; Groß, T. Awareness of challenges and barriers in integrating cultural values into cybersecurity is limited, necessitating increased awareness. *Comput. Secur.* **2018**, *74*, 210–224. [CrossRef]
48. Veiga, A.D.; Martins, N. Defining and identifying dominant information security cultures and subcultures highlights the need for cultural intervention in cybersecurity policies. *Comput. Secur.* **2017**, *70*, 72–94. [CrossRef]
49. Nkongolo, P.M.; Tan, J.; Wethal, P.M. Cultural awareness and training are essential components of cybersecurity professions, enhancing the ability to address diverse threats. *J. Cybersecur. Priv.* **2023**, *3*, 101–115.
50. Veiga, A.D. Comparing information security cultures of employees emphasises the importance of reading and understanding security policies. *Inf. Comput. Secur.* **2016**, *24*, 134–151.
51. Chakraborty, A.; Biswas, A.; Khan, A.K. *Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation*; Springer Nature: Berlin, Germany, 2023; pp. 3–25. [CrossRef]