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

Md. Rajib Hasan *, Nurul I. Sarkar *, Noor H. S. Alani, Raymond Lutui

Posted Date: 27 September 2024

doi: 10.20944/preprints202409.2174.v1

Keywords: Cyber Edge; Cultural Integration; Cybersecurity; Aotearoa-New Zealand; Cybersecurity Resilience; Diversity; Cultural Competency; Inclusive Strategies

Article

Cyber Edge: Current State of Cyber Security 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, New Zealand
[2] Department of Computer Science and Software Engineering, Auckland University of Technology, New Zealand
* Correspondence: nurul.sarkar@aut.ac.nz; rhasan@eit.ac.nz

Abstract: As Aotearoa-New Zealand faces increasing cyber threats, this paper comprehensively analyses the nation's current cybersecurity landscape, revealing novel opportunities and challenges. Through an interdisciplinary approach, the study integrates social, cultural, and technological dimensions—providing a fresh perspective that has been underexplored in previous research. A key focus is integrating cultural values, particularly those of the indigenous Māori, into cybersecurity practices. This not only strengthens the effectiveness and trustworthiness of security measures but also fosters a more inclusive and resilient digital environment, demonstrating our deep respect for the unique contributions of Māori culture. Additionally, this paper introduces critical insights into the country's cybersecurity talent gap, with a special focus on the challenges of developing and retaining cybersecurity expertise in remote regions. Our study also uncovers underexplored opportunities for cross-sector collaboration between private enterprises, government agencies, and indigenous communities, promoting an inclusive and resilient approach to cybersecurity. By positioning Aotearoa-New Zealand as a potential leader in regional cybersecurity innovation, we provide forward-looking recommendations that leverage its distinctive cultural and technological strengths. This research contributes fresh insights to the global discourse on cybersecurity, offering practical strategies tailored to the specific needs of smaller nations.

Keywords: Cyber Edge; Cultural Integration; Cybersecurity; Aotearoa-New Zealand; Cybersecurity Resilience; Diversity; Cultural Competency; Inclusive Strategies

1. Introduction

In the modern digital era, the importance of cyber security knowledge cannot be overstated, as the increasing reliance on technology and the internet has made individuals, including indigenous Māori people in New Zealand (known as Aotearoa-New Zealand), more vulnerable to various cyber threats. One of the primary reasons why cyber security 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 [22]. Furthermore, cyber security knowledge is vital for safeguarding the integrity of businesses and organizations, as cyber-attacks pose a significant threat to their economic stability. The New Zealand government, for instance, is estimated to lose a staggering NZD 257 million per year to cybercrime [2,32], 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 emphasizes community and collective responsibility. This collective mindset can be utilized to create a sense of shared responsibility for cybersecurity within the country [7,13,15].

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

 doi:10.20944/preprints202409.2174.v

[17]. By bridging this divide, the country can create a more inclusive and resilient cybersecurity ecosystem [30]. One key aspect of this approach is emphasizing relationships with the community and demonstrating leadership in repositioning culture at the heart of everything [13]. 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 [13].

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. [30] By working together, stakeholders can share information, best practices, and resources, strengthening the country's cybersecurity posture [7,28].

Additionally, the government plays a crucial role in enabling a cultural intervention approach [9]. 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 prioritizing cybersecurity nationally, Aotearoa New Zealand, can create a secure and resilient digital environment.

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.

Finally, the intervention framework with a cultural approach provides a systematic and evidence-based approach to improving cyber security knowledge among the Māori people. By tailoring interventions to the specific needs and cultural context of the Māori community, policymakers and organizations can effectively address the current challenges and empower the Māori to protect themselves online [13]. Involving key stakeholders and evaluating the impact of interventions is crucial to achieving sustainable and long-term improvements in cyber security knowledge among the Māori people [13].

1.1. Research Challenges

The challenge lies in effectively integrating diverse cultural values, such as those of the Māori, 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 research questions.

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

The main rationale behind this question is cultural values significantly impact cybersecurity practices in Aotearoa-New Zealand, particularly through the integration of Māori cultural principles. The research underscores the importance of incorporating cultural perspectives into cybersecurity strategies to enhance their effectiveness, trust, and engagement.

Māori culture, with its emphasis on community and collective responsibility, is highlighted as playing a unique and crucial role in shaping cybersecurity practices. This cultural approach fosters a sense of shared responsibility for cybersecurity, which is essential for creating a resilient digital environment. Furthermore, the integration of cultural values helps bridge the digital divide by

 doi:10.20944/preprints202409.2174.v

ensuring equal access to digital resources and knowledge, making cybersecurity measures more inclusive. The digital divide is a significant issue in Aotearoa-New Zealand, particularly among indigenous communities. By exploring the role of cultural values in cybersecurity, this research aims to highlight the importance of inclusive strategies that ensure equal access to digital resources and cybersecurity knowledge, thereby helping to bridge this divide.

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

This question emerges from a deep understanding of the unique challenges facing the country. In Aotearoa-New Zealand, the digital divide is more than just a technological issue; it's a reflection of broader societal inequalities, particularly among indigenous Māori communities and other marginalized groups. As we move further into a digital age, the gap between those who have access to technology and those who do not is becoming increasingly significant. This divide is*n't* just about having the latest devices or high-speed internet; i*t's* about access to opportunities, education, and the ability to participate fully in a rapidly changing world. For many in Aotearoa-New Zealand, particularly in rural or underserved areas, the lack of access to digital resources and knowledge means being left behind in critical aspects of life, from education and employment to civic engagement.

By exploring what can be done to provide equal access, we are essentially asking how we can create a more equitable society, where everyone, regardless of their background or location, has the opportunity to benefit from the digital world. This question is not just about technology; i*t's* about social justice, community empowerment, and the future of Aotearoa-New Zealand as a whole.

1.2. 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 summarized as follows.

- We provide research and valuable insights into the integration of 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. Literature Review

2.1. Research Area on Cyber Security in Cultural Intervention

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

 doi:10.20944/preprints202409.2174.v

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

Reference	Research area
[21]	Integrating cultural values into cybersecurity practices enhances security and resilience.
[3]	Cultural views, including those in e-learning risk analysis, can be leveraged to enhance cybersecurity efforts.
[29]	Cultural dimensions significantly correlate with cybersecurity development, suggesting a need for integrating cultural perspectives into cybersecurity practices.
[1]	Towards an intercultural approach to information security, we emphasise the importance of cultural awareness and training.
[37]	Examining the relationship between culture and information security awareness highlights the necessity of cultural integration in cybersecurity.
[31]	Variations in information security cultures across professions necessitate understanding these differences for effective cybersecurity practices.
[16]	Cultural and psychological factors significantly impact cybersecurity practices and user behaviour.
[34]	Developing a cybersecurity culture is crucial for effective practices and resilience; more comprehensive education and awareness programs are needed.
[35]	Comparing information security cultures of employees emphasises the importance of reading and understanding security policies.
[36]	Defining and identifying dominant information security cultures and subcultures highlights the need for cultural intervention in cybersecurity policies.
[6]	Awareness of challenges and barriers in integrating cultural values into cybersecurity is limited, necessitating increased awareness.
[27]	Inter-organizational knowledge sharing drives national cybersecurity awareness, but challenges remain in integrating cultural values.
[22]	Family member's awareness of cyber-security concepts and their correlation with the precautionary procedures taken against cyber-attacks during the Coronavirus pandemic .
[25]	Cultural awareness and training are essential components of cybersecurity professions, enhancing the ability to address diverse threats.
[19]	Cybersecurity awareness measurement models must incorporate cultural dimensions for effectiveness.
[18]	Managing cognitive and cultural diversity in global IT teams enhances cybersecurity collaboration and information sharing.
[23]	Technology-assisted cultural diversity learning is crucial for equipping learners with the necessary skills for cybersecurity collaboration.
[5]	Defining cybersecurity must include organisational, economic, social, and political factors tied to cultural dimensions.
[13]	Community engagement and inclusive policy development are paramount for fostering cultural awareness of cybersecurity.
[10]	Cultural safety and competency are required to achieve effective cybersecurity practices.
[24]	Building indigenous knowledge and integrating cultural elements into cybersecurity is crucial for effective practices.
[14]	Critical success factors for cybersecurity include incorporating cultural values and perspectives.
[24]	Critical elements of an information security culture include cultural dimensions, which improve communication and education.
[12]	An annotated bibliography on information security highlights the need for cultural integration in cybersecurity.

 doi:10.20944/preprints202409.2174.v

[28]	A comparative study of national cybersecurity strategies underscores the importance of cultural diversity and joint cyber threat-sharing centres.
[20]	The global pandemic's influence on cybersecurity highlights the need for a robust cybersecurity culture.
[4]	Protecting information with cybersecurity involves addressing cultural dimensions for effective practices.
[11]	The future cybersecurity workforce requires going beyond technical skills to include cultural competency.
[38]	Cultural diversity in multi-national ICT organisations enhances cybersecurity collaboration.

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

Table 2 summarizes 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	**Integrating Cultural Values in Cybersecurity Practices:** • Enhances user compliance and trust [1,3,16,21,29,31,37]. • Improves security resilience by making measures more relevant and acceptable to diverse groups [1,5,11,30,34]. • Facilitates better user engagement and compliance [14,16,24,29,34]. **Cultural Diversity in Cybersecurity Collaboration:** • Enhances problem-solving and innovation [16,18]. • Improves information sharing and threat intelligence [5,33,38]. **Cybersecurity Culture:** • Essential for enhancing security posture and fostering proactive behaviours [7,14,20,28]. • Contributes to better risk management and organisational resilience [4].
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 [27]. **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.
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 programs that address specific cultural factors influencing cybersecurity behaviours. **Conducting Region-Specific Studies:**

 doi:10.20944/preprints202409.2174.v

- 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.

2. Methods

The study employs a mixed-methods approach, utilizing a survey administered to cybersecurity professionals across Aotearoa New Zealand. Based on the literature study 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.

Figure 1. Technology and Tools used in Literature Review (Image drawn at https://whimsical.com/).

3. 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 programs. 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).

3.1. 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

 doi:10.20944/preprints202409.2174.v

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.

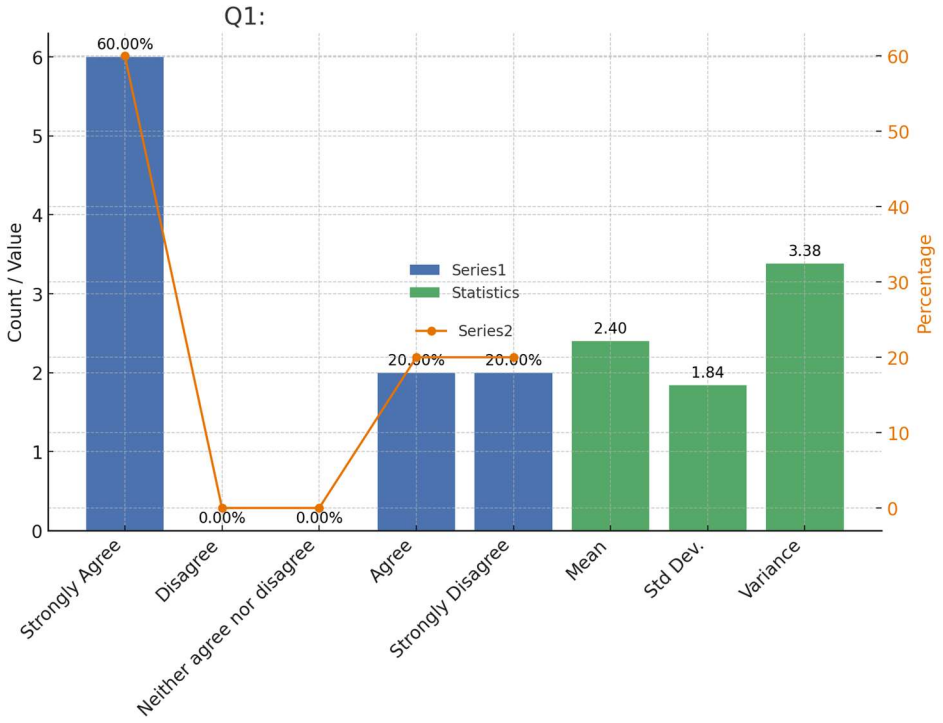

Figure 2. Respondents' opinions on the effectiveness of integrating cultural values and perspectives.

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.

3.2. 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 organizations 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

 doi:10.20944/preprints202409.2174.v

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.

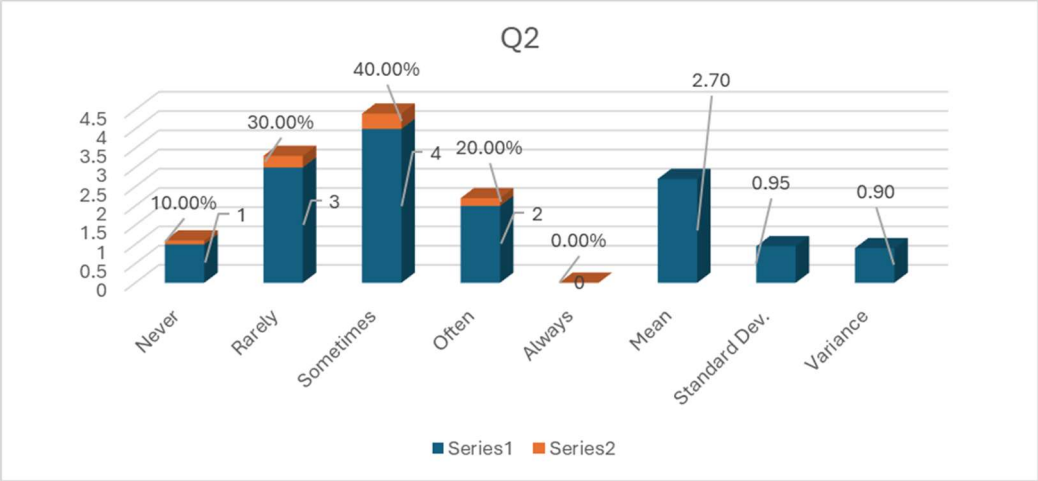

Figure 3. Impacted cybersecurity where cultural knowledge or practices have positively.

The responses indicate a varied experience among the participants regarding the influence of cultural knowledge on cybersecurity. A 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 organizations.

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. Organizations 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 maximise 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.

3.3. 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.

 doi:10.20944/preprints202409.2174.v

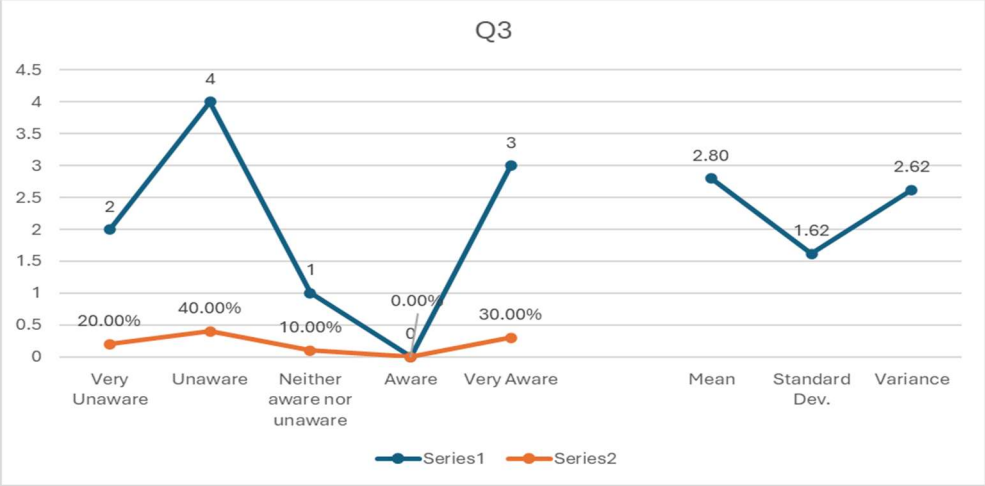

Figure 4. Awareness of cultural and linguistic diversity and its potential impact on cybersecurity.

A notable 20.00% of respondents indicated they were unaware of their organization'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 recognizing nor dismissing the significance of cultural and linguistic diversity. Notably, no respondents identified themselves as "Aware," while 30.00% of respondents expressed 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 organizations 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.

3.4. 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 5 depicts 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. 50.00% agreed that specific actions or strategies could effectively incorporate cultural values and perspectives. 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.

 doi:10.20944/preprints202409.2174.v

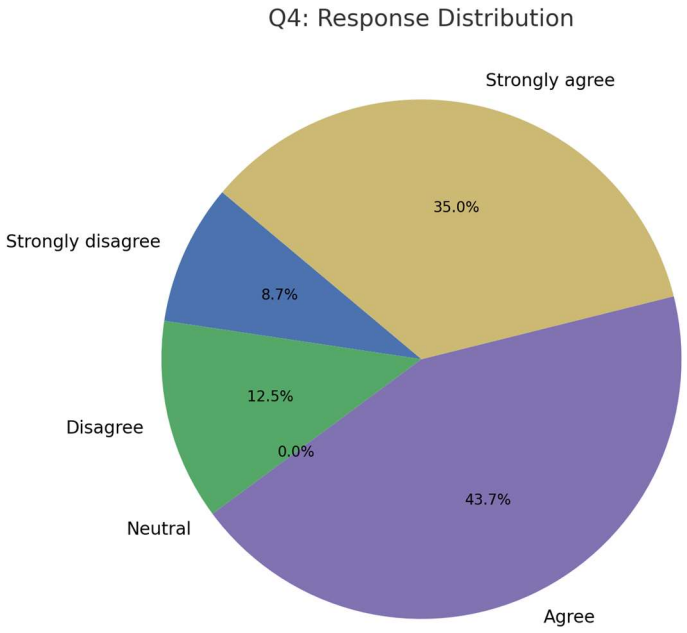

Figure 5. Require actions or strategies to be implemented to incorporate cultural values and perspectives in cybersecurity effectively.

The mean score of 4.10 suggests a generally positive outlook among respondents regarding implementing 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 analyzed 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 the participants regarding integrating 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, organizations and communities can enhance their cybersecurity posture by embracing diversity and leveraging cultural insights effectively.

3.5. 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 recognized 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 categorized from "Strongly Disagree" to "Strongly Agree".

 doi:10.20944/preprints202409.2174.v

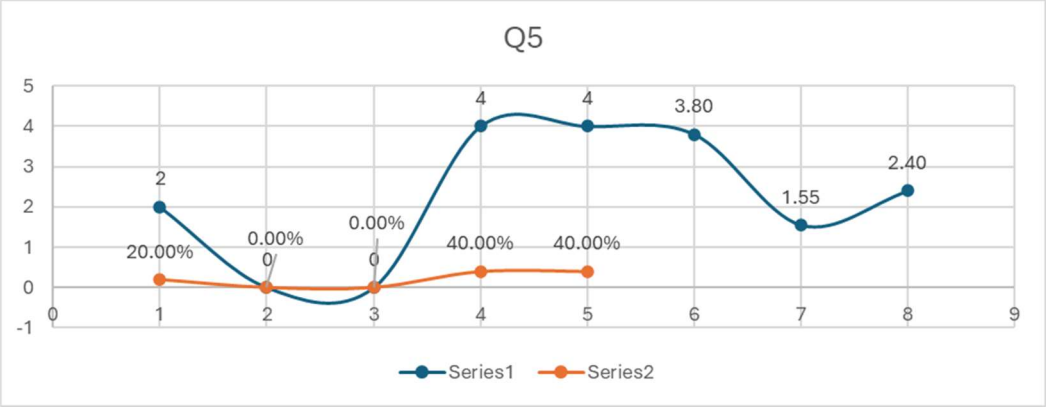

Figure 6. Require cultural awareness and training in cybersecurity professions.

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. 40.00% agreed that cultural awareness and training are necessary. 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 emphasize 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 prioritizing these aspects, organizations can better equip cybersecurity professionals to navigate an increasingly diverse and complex threat environment.

3.6. 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 categorized 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.

 doi:10.20944/preprints202409.2174.v

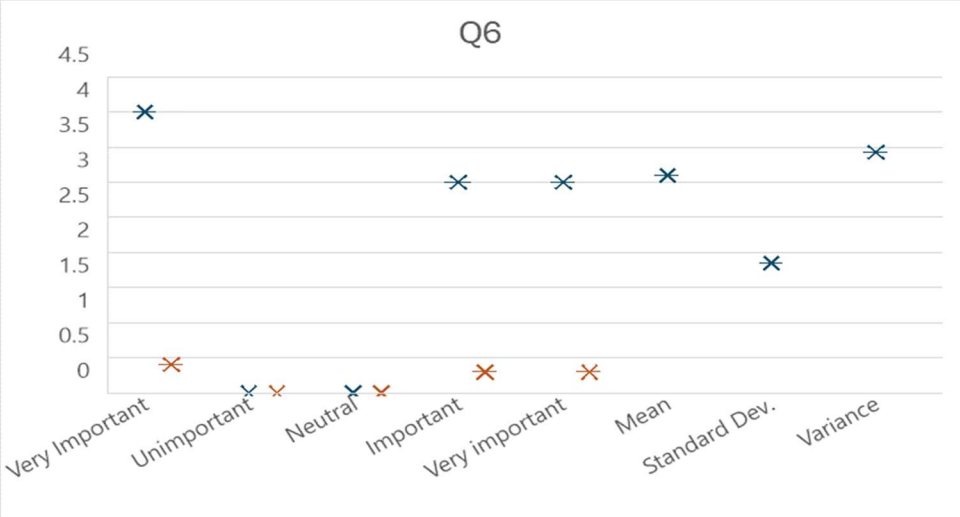

Figure 7. Importance of cybersecurity professionals to understand the cultural context.

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 defenses and fosters a more inclusive and responsive organizational culture. This study highlights a significant consensus among cybersecurity professionals regarding the importance of understanding cultural context in their roles. By prioritizing cultural awareness, organizations can better mitigate cybersecurity risks and build stronger relationships with the communities they serve.

3.7. 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 organizational 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 categorized 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. 0.00% of respondents disagreed. 0.00% of respondents were neutral. 33.33% of respondents agreed. 55.56% of respondents strongly agreed.

 doi:10.20944/preprints202409.2174.v

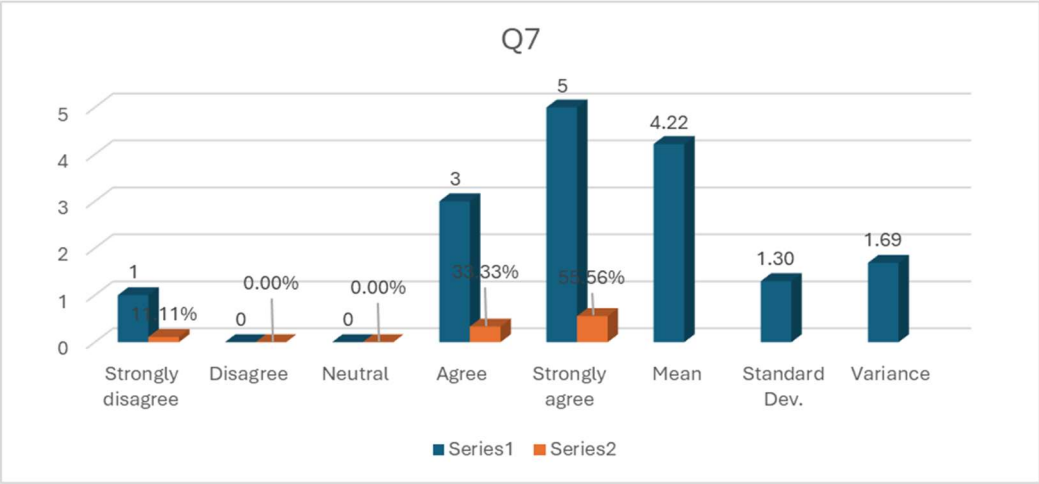

Figure 8. Identifying cultural intervention can contribute to developing effective cybersecurity policies and practices.

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, organizations can enhance their resilience and responsiveness to diverse threats.

3.8. 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 categorized from "Very Unaware" to "Very Aware".

Figure 9 shows that 10.00% of respondents indicated they were unaware of the challenges and barriers. 60.00% of respondents were neutral, and unaware of the challenges. No respondents identified themselves as aware. 20.00% of respondents indicated they knew the obstacles and barriers.

 doi:10.20944/preprints202409.2174.v

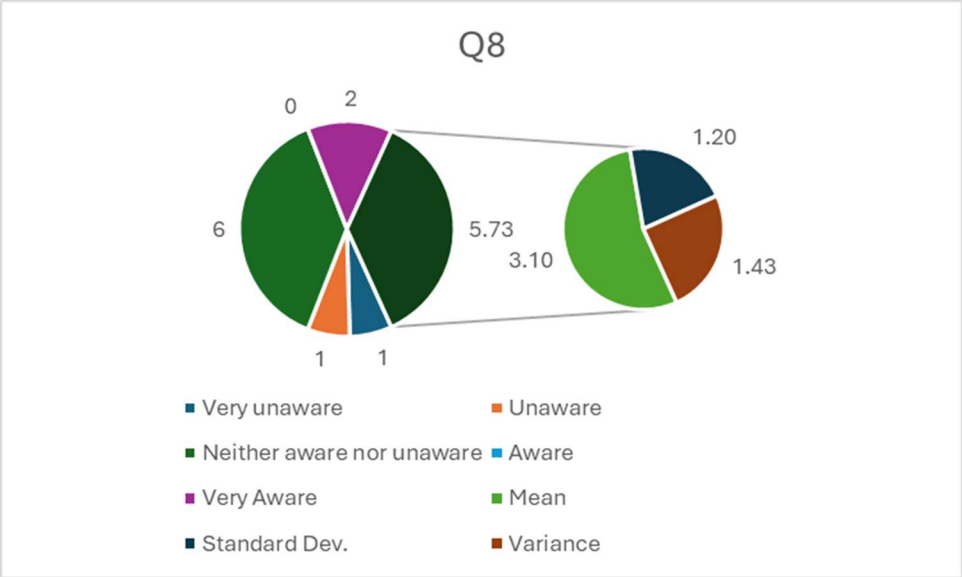

Figure 9. Aware of any challenges or barriers when incorporating cultural values and perspectives in cybersecurity.

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. Recognizing 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. Organizations can develop more effective and inclusive cybersecurity policies and practices by increasing awareness and addressing these challenges.

3.9. 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 organizations or communities. A survey was administered to cybersecurity professionals to assess their experiences with challenges related to incorporating cultural values and attitudes. Responses were categorized 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.

 doi:10.20944/preprints202409.2174.v

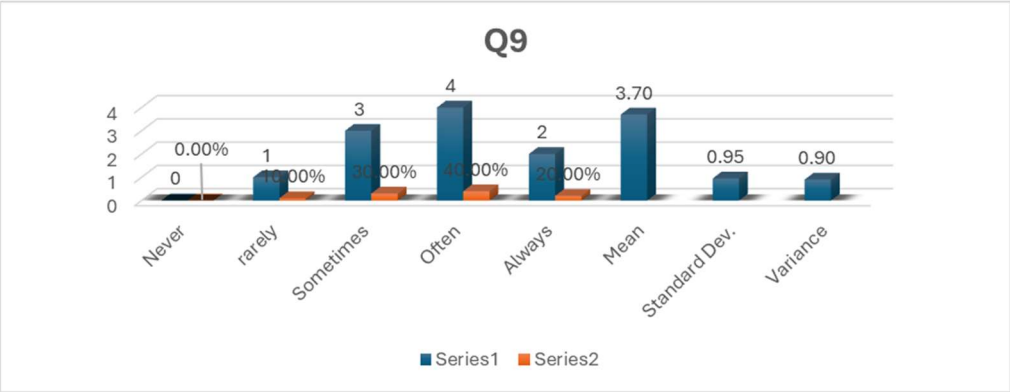

Figure 10. Challenges or issues encountered in incorporating cultural values and perspectives in cybersecurity.

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. Organizations can create more effective and culturally sensitive cybersecurity strategies by addressing these challenges through targeted training, inclusive policy development, and community engagement.

3.10. 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) consider cultural diversity very important. 12.5% (1 respondent) consider it unimportant. 12.5% (1 respondent) are neutral, as illustrated in Figure 10.

 doi:10.20944/preprints202409.2174.v

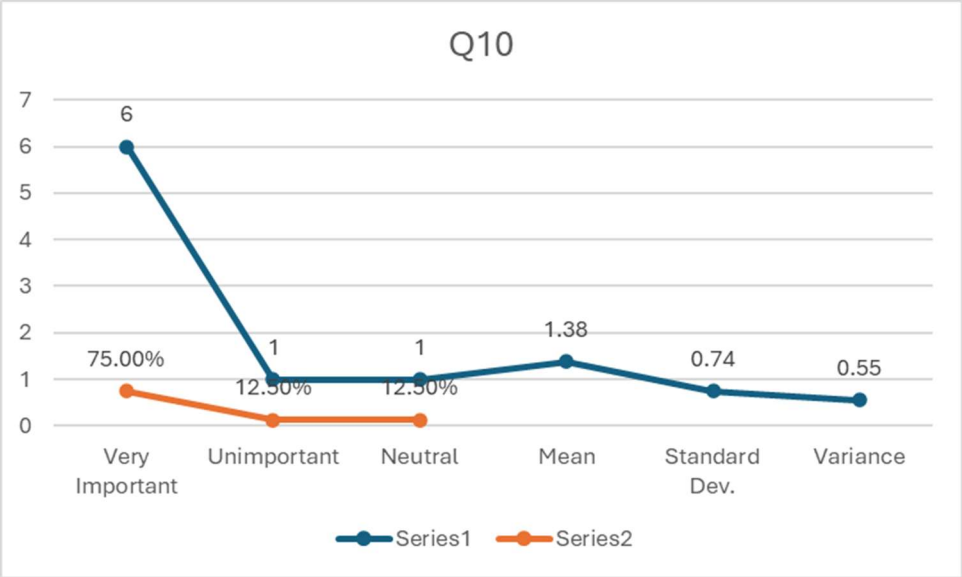

Figure 11. Role of cultural diversity in cybersecurity.

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 cybersecurity 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.

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

Figure 12 is a complex, multi-layered doughnut chart that visualizes 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.

 doi:10.20944/preprints202409.2174.v

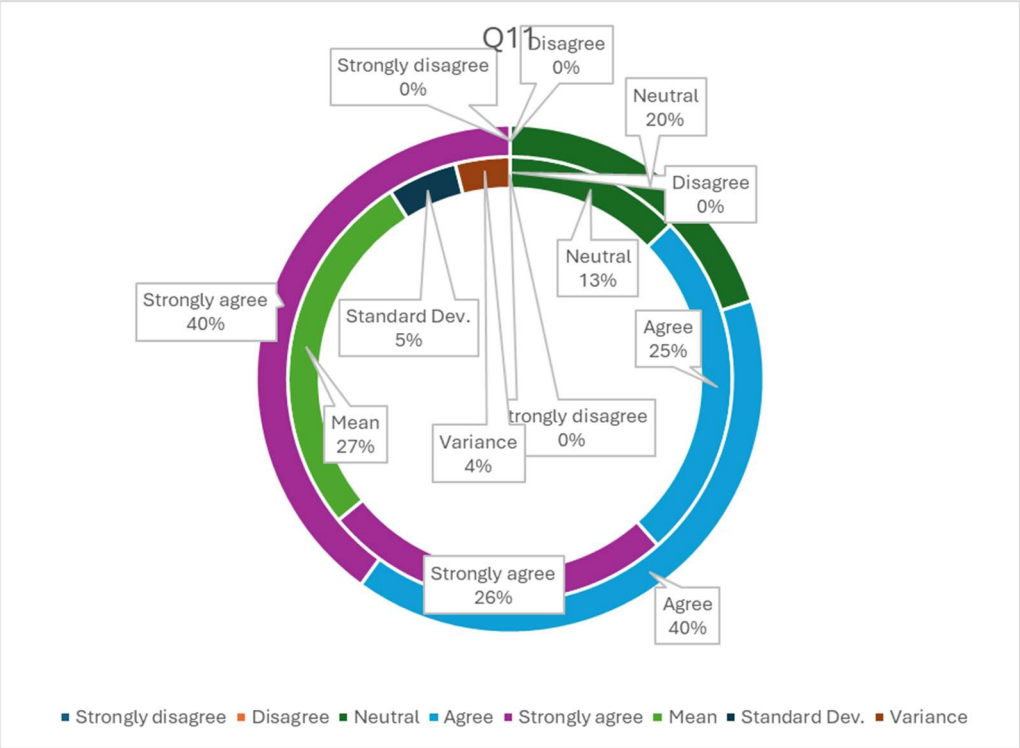

Figure 12. Status of Cyber Security culture and Information Security Culture.

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 recognize 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 emphasize 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 organizations, where cybersecurity requires more specialized 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 organizations and policymakers as they develop strategies and frameworks to enhance their security postures. Recognizing these cultural differences can lead to more targeted and adequate security measures tailored to address each field's unique challenges and dynamics.

3.12. 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

 doi:10.20944/preprints202409.2174.v

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. Localized 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.

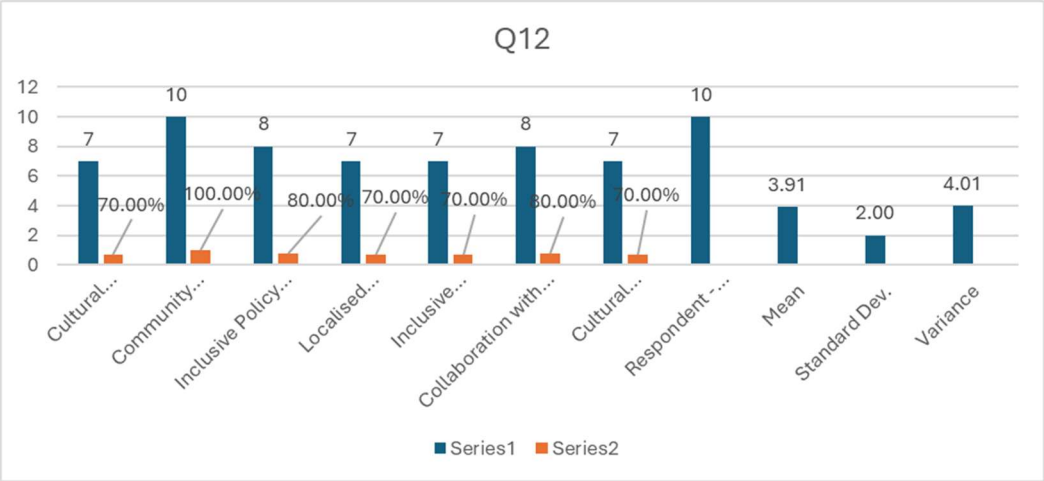

Figure 13. Strategies or initiatives to promote cultural awareness and inclusivity in cybersecurity.

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.

3.13. 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.

 doi:10.20944/preprints202409.2174.v

Figure 14 shows that cultural competency training (100%) provides comprehensive training programs to enhance the cultural competency of cybersecurity professionals. This includes educating them on different groups' cultural norms, values, and communication 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 programs tailored to local cultural contexts. This helps to improve engagement and understanding of cybersecurity principles among diverse populations. Inclusive Design & 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.

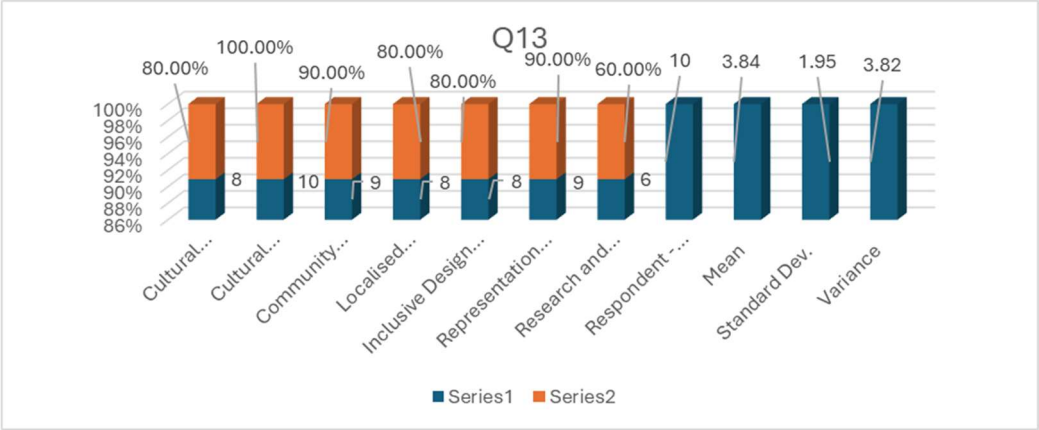

Figure 14. Steps to bridge the gap between cultural practices and cybersecurity.

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.

 doi:10.20944/preprints202409.2174.v

3.14. 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 14 visualizes 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 15, 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, organizations 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 recognizing 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.

 doi:10.20944/preprints202409.2174.v

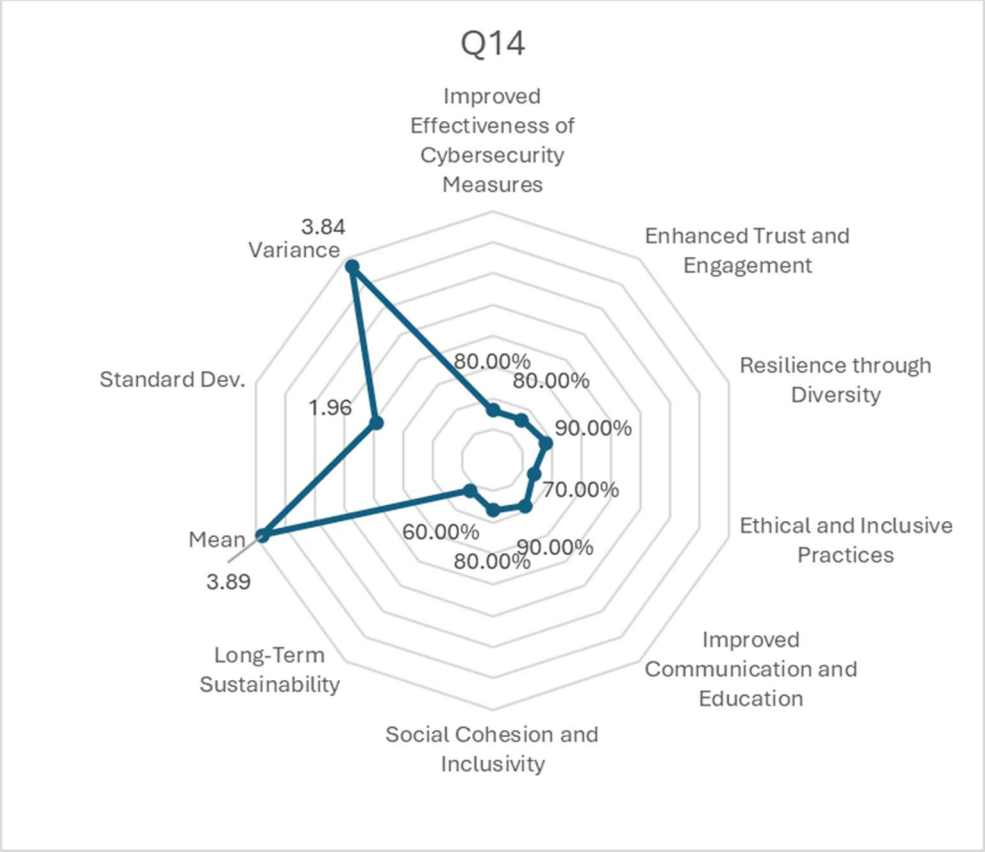

Figure 15. Potential benefits of incorporating cultural values and perspectives in cybersecurity practices.

Mean 3.89, indicating the average number of benefits recognized 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.

3.15. Q15 Is Fostering a Cyber Security 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 shout to 100% that raising cyber security 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.

 doi:10.20944/preprints202409.2174.v

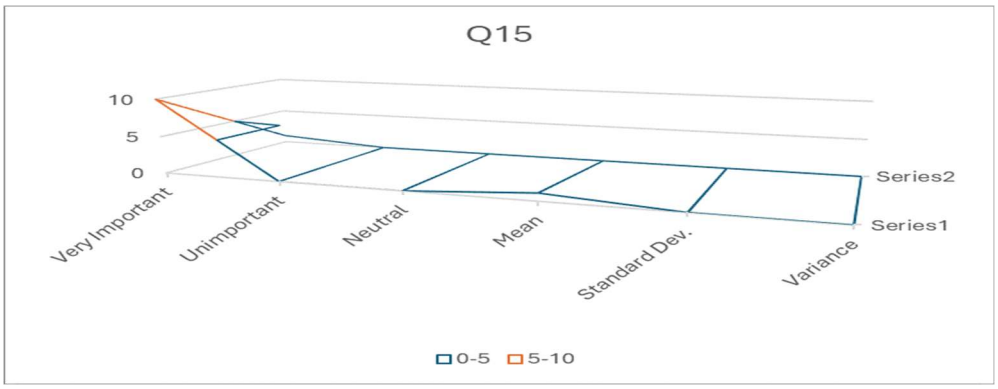

Figure 16. Fostering cyber security culture in Aotearoa-New Zealand vital for effective cybersecurity practices.

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

The bar chart in Figure 16 represents responses to a survey question about fostering a cybersecurity culture in Aotearoa-New Zealand, emphasizing 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 cyber security culture in Aotearoa-New Zealand could contribute to the overall strength of the nation's cybersecurity infrastructure.

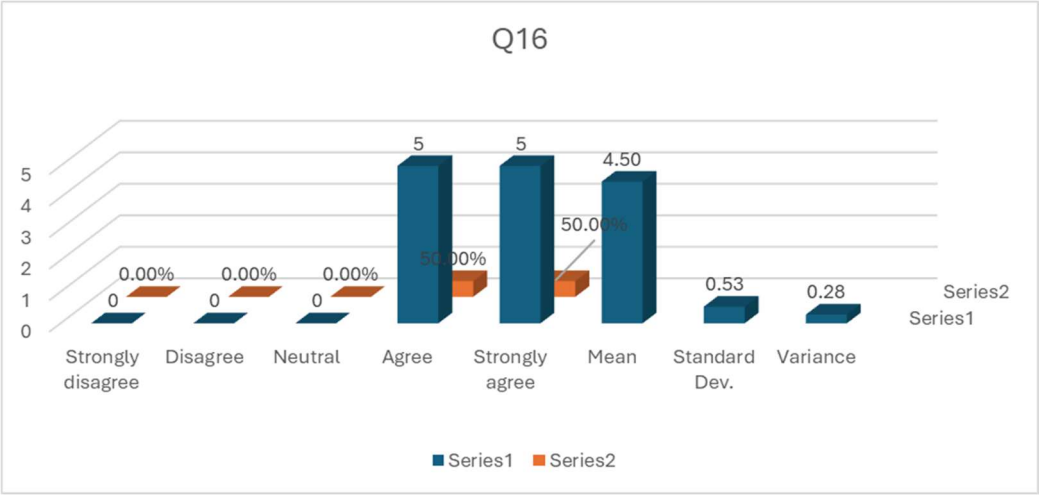

Figure 17. Belief in cyber security culture can contribute to overall resilience.

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.

 doi:10.20944/preprints202409.2174.v

4. Results and Validation

4.1. 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.

4.2. 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 recognized 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.

4.3. 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.

4.4. 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.

4.5. 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

 doi:10.20944/preprints202409.2174.v

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.

4.6. Importance of Understanding Cultural Context

All respondents recognize 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 recognize 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.

4.7. 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.

4.8. Awareness of Challenges

Respondents exhibit moderate awareness of challenges associated with incorporating cultural values into cybersecurity, 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 recognizing 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.

4.9. 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.

 doi:10.20944/preprints202409.2174.v

4.10. 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 recognize 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.

4.11. 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. Recognizing 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.

5. Discussion

5.1. 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 organizations respect and acknowledge different cultural values, fostering an environment where stakeholders feel valued and are more likely to adhere to security protocols. Moreover, diversity brings varied perspectives, which can strengthen resilience by identifying and addressing a broader range of threats. To fully harness these benefits, organizations should prioritize 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 organizational culture.

5.2. Addressing Challenges

The frequent challenges reported by respondents emphasize 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 localized cybersecurity education, which tailors training and awareness programs to different communities' specific cultural contexts and needs. By implementing these strategies, organizations can create a more inclusive and effective cybersecurity environment that leverages the strengths of cultural diversity.

 doi:10.20944/preprints202409.2174.v

5.3. 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 emphasizing cultural diversity. Recognizing 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.

6. Conclusion

In this paper we addressed the following two research questions: (i) what effect do cultural values have on cybersecurity practices in Aotearoa New Zealand? and (ii) what can be done to provide equal access to digital resources in bridging the digital divide in New Zealand? This study has demonstrated the critical role of cultural values in developing effective cybersecurity practices in Aotearoa New Zealand. We found that adopting cultural diversity can help organizations to enhance security measures, foster collaboration, and build resilient cybersecurity infrastructures. Integrating diverse cultural perspectives contributes to more robust and adaptable security strategies, promoting stakeholder trust and cooperation. Developing a comprehensive cybersecurity framework to identify the specific cultural activities and to study their impact on cybersecurity practices in the society and organizations of New Zealand is suggested as future research direction.

References

1. Andrés, R., & Plachkinova, M. (2018). Towards an intercultural approach to information security, we emphasise the importance of cultural awareness and training. *Journal of Global Information Technology Management*, 21(1), 62-78.
2. Aljuhami, A. M., & Bamasoud, D. M. (01 2021). Cyber Threat Intelligence in Risk Management. Science and Information Organization, 12(10). doi:10.14569/ijacsa.2021.0121018
3. Alwi, N. H. M., & Fan, I.-S. (2012). Cultural views, including those in e-learning risk analysis, can be leveraged to enhance cybersecurity efforts. Computers & Education, 58(3), 692-702. https://doi.org/10.1016/j.compedu.2011.09.016
4. Borky, J. M., & Bradley, T. H. (2018). Protecting information with cybersecurity involves addressing cultural dimensions for effective practices. *Journal of Strategic Security*, 11(3), 59-76.
5. Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity must include organisational, economic, social, and political factors tied to cultural dimensions. *Technology Innovation Management Review*, 4(10), 13-21.
6. Coopamootoo, K., & Groß, T. (2018). Awareness of challenges and barriers in integrating cultural values into cybersecurity is limited, necessitating increased awareness. *Computers & Security*, 74, 210-224. https://doi.org/10.1016/j.cose.2018.01.016
7. Curtis, R., Davies, H., & Cameron, J. (2019). Cultural safety and competency are required to achieve effective cybersecurity practices. *Cyberpsychology, Behavior, and Social Networking*, 22(5), 348-356. https://doi.org/10.1089/cyber.2018.0635
8. Chakraborty, A., Biswas, A., & Khan, A. K. (01 2023). Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation. Springer Nature, pp. 3–25. doi:10.1007/978-3-031-12419-8_1
9. Chang, L. Y.-C., & Coppel, N. (10 2020). Building cyber security awareness in a developing country: Lessons from Myanmar. Elsevier BV, 97, 101959–101959. doi:10.1016/j.cose.2020.101959
10. Curtis, E., Jones, R., Tipene-Leach, D., Walker, C., Loring, B., Paine, S., & Reid, P. (11 2019). Why cultural safety rather than cultural competency is required to achieve health equity: a literature review and recommended definition. BioMed Central, 18(1). doi:10.1186/s12939-019-1082-3
11. Dawson, M., & Thomson, R. (2018). The future cybersecurity workforce requires going beyond technical skills to include cultural competency. *Journal of Cybersecurity Education, Research and Practice*, 4(1), 3.
12. Feary, M. (2021). An annotated bibliography on information security highlights the need for cultural integration in cybersecurity. *Library & Information Science Research*, 43(4), 101118. https://doi.org/10.1016/j.lisr.2021.101118
13. Fraser, S., McKay, G., & Stalker, C. (2020). Community engagement and inclusive policy development are paramount for fostering cultural awareness in cybersecurity. *Government Information Quarterly*, 37(2), 101384. https://doi.org/10.1016/j.giq.2019.101384

14. Frei, S., May, M., & Fiedler, M. (2013). Critical success factors for cybersecurity include incorporating cultural values and perspectives. *Journal of Computer Security*, 21(6), 839-864. https://doi.org/10.3233/JCS-130500
15. Habib, A., Densmore-James, S., & Macfarlane, S. (06 2013). A Culture of Care: The Role of Culture in Today's Mainstream Classrooms. Taylor & Francis, 57(3), 171–180. doi:10.1080/1045988x.2013.798777
16. Halevi, T., Memon, N., Lewis, J A., Kumaraguru, P., Arora, S., Dagar, N., Aloul, F., & Chen, J. (2016, November 28). *Cultural and psychological factors in cyber-security*. https://doi.org/10.1145/3011141.3011165
17. Hammond, S. P., Polizzi, G., & Bartholomew, K. J. (09 2022). Using a socio-ecological framework to understand how 8–12-year-olds build and show digital resilience: A multi-perspective and multimethod qualitative study. Springer Science+Business Media, 28(4), 3681–3709. doi:10.1007/s10639-022-11240-z
18. Jablokow, K. W., & Myers, C. R. (2010). Managing cognitive and cultural diversity in global IT teams enhances cybersecurity collaboration and information sharing. *IEEE Transactions on Engineering Management*, 57(2), 250-265. https://doi.org/10.1109/TEM.2009.2033040
19. Khan, H. U., Rehman, M., & Kim, D. (2020). Cybersecurity awareness measurement models must incorporate cultural dimensions for effectiveness. *International Journal of Information Management*, 50, 202-214. https://doi.org/10.1016/j.ijinfomgt.2019.05.024
20. Khatri, M., Choubey, M., & Sharma, R. (2023). The global pandemic's influence on cybersecurity highlights the need for a robust cybersecurity culture. *Journal of Information Security and Applications*, 70, 103012. https://doi.org/10.1016/j.jisa.2022.103012
21. Kruger, H. A., Drevin, L., & Steyn, T. (2011). Integrating cultural values into cybersecurity practices enhances security and resilience. Journal of Information Warfare, 10(2), 43-54.
22. Malibari, N. (2021, January 1). 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, 120-129. https://doi.org/10.5937/intrev2102122m
23. Momo, F. (2022). Building indigenous knowledge and integrating cultural elements into cybersecurity is crucial for effective practices. *Journal of Information Security and Applications*, 67, 102932. https://doi.org/10.1016/j.jisa.2022.102932
24. Nel, L., & Drevin, L. (2019). Key elements of an information security culture include cultural dimensions, which improve communication and education. *Computers & Security*, 84, 1-10. https://doi.org/10.1016/j.cose.2019.03.009
25. Nkongolo, P. M., Tan, J., & Wethal, P. M. (2023). Cultural awareness and training are essential components of cybersecurity professions, enhancing the ability to address diverse threats. *Journal of Cybersecurity and Privacy*, 3(1), 101-115.
26. McIlwraith, A. (2006). Information security and employee behaviour must be addressed through cultural considerations to reduce risks. *Information Security Technical Report*, 11(1), 32-44. https://doi.org/10.1016/j.istr.2006.01.001
27. Persadha, H. R., Noor, T. H. A., & Mohtar, W. A. W. (2016). Inter-organizational knowledge sharing drives national cybersecurity awareness, but challenges remain in integrating cultural values. *Journal of Information Security and Applications*, 30, 79-87. https://doi.org/10.1016/j.jisa.2016.04.002
28. Odebade, A. A., & Benkhelifa, E. (2023). A comparative study of national cybersecurity strategies underscores the importance of cultural diversity and joint cyber threat-sharing centres. *Journal of Cybersecurity Research*, 10(1), 45-63. https://doi.org/10.1016/j.jcsr.2022.102512
29. Onumo, E. G., Briggs, J., & Adedoyin, A. (2017). Cultural dimensions significantly correlate with cybersecurity development, suggesting a need for integrating cultural perspectives into cybersecurity practices. *Information & Computer Security*, 25(5), 572-589.
30. Onwubiko, C., & Ouazzane, K. (02 2022). Multidimensional Cybersecurity Framework for Strategic Foresight. 6(1), 46–77. doi:10.22619/ijcsa.2021.100137
31. Ramachandran, S., Rao, U., & Narayanan, V. (2013). Variations in information security cultures across professions necessitate understanding these differences for effective cybersecurity practices. *International Journal of Information Management*, 33(5), 767-776. https://doi.org/10.1016/j.ijinfomgt.2013.02.003
32. Sarker, I H., Kayes, A S M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020, July 1). Cybersecurity data science: an overview from machine learning perspective. Springer Science+Business Media, 7(1). https://doi.org/10.1186/s40537-020-00318-5
33. Shadiev, R., Hwang, G.-J., & Liu, T.-C. (2023). Technology-assisted cultural diversity learning is crucial for equipping learners with the necessary skills for cybersecurity collaboration. *Educational Technology Research and Development*, 71(1), 39-54. https://doi.org/10.1007/s11423-022-10113-9
34. Uchendu, A., Niekerk, J. V., & Futcher, L. (2021). Developing a cybersecurity culture is crucial for effective practices and resilience; more comprehensive education and awareness programs are needed. *Computers & Security*, 102, 102129. https://doi.org/10.1016/j.cose.2020.102129
35. Veiga, A. D. (2016). Comparing information security cultures of employees emphasises the importance of reading and understanding security policies. *Information & Computer Security*, 24(2), 134-151.

 doi:10.20944/preprints202409.2174.v

36. Veiga, A. D., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures highlights the need for cultural intervention in cybersecurity policies. *Computers & Security*, 70, 72-94. https://doi.org/10.1016/j.cose.2017.05.004vvv
37. Wiley, A., Ross, A., & Pye, R. (2020). Examining the relationship between culture and information security awareness highlights the necessity of cultural integration in cybersecurity. *Computers & Security*, 94, 101857. https://doi.org/10.1016/j.cose.2020.101857
38. Zafar, H., Ko, M., & Osei-Bryson, K. M. (2017). Cultural diversity in multi-national ICT organisations enhances cybersecurity collaboration. *Journal of Global Information Technology Management*, 20(2), 57-76. https://doi.org/10.1080/1097198X.2017.1309514