Scientific and Practical Cyber Security Journal (SPCSJ) 8(2): 19 – 31 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

STRENGTHENING WORKPLACE CYBER RESILIENCE: BRIDGING THE DIVIDE BETWEEN PERCEPTION AND REALITY

Kgantshe Tau (BCom)[1], Rodney Mushininga (PhD) [2]
[1]Mancosa, 26 Samora Machel Street. Durban 4001, South Africa
[2]School of Information Technology, The Independent Institute of Education, IIEMSA, Johannesburg, South Africa

ABSTRACT: As digital transformation accelerates across industries, effective cyber resilience is paramount for maintaining business operations amid evolving cyber threats. The challenge is that the current research shows a lack of alignment between executive perceptions of preparedness and realities assessed by technical teams. To address this perception gap and strengthen organizational cyber resilience, this paper explores challenges and opportunities across key dimensions. A literature review reveals workforce development as a strategic priority. While some studies emphasize crisis management training, retention strategies are also vital for maintaining skilled cybersecurity talent over the long term. Disconnects also exist between conceptual frameworks and practical implementation, highlighting the need for shared understanding across leadership and practitioners. Standardized metrics are likewise needed to benchmark resilience effectiveness within and across sectors.
The paper utilizes a quantitative survey design to collect data from business leaders and cybersecurity professionals. Targeting these stakeholder groups from diverse industries facilitates statistically analyzing relationships between variables like training effectiveness and perception gaps. Key findings reveal notable perception gaps between leadership and technical roles regarding readiness. Training programs also exhibit uneven implementation and impact. Workforce retention efforts lack awareness, suggesting room for improvement. Frameworks receive mixed feedback on consistency and adaptability to technological change. To bridge divides, a holistic strategy is recommended encompassing unified understanding and planning; dynamic training and innovative retention; agile frameworks integrating emerging technologies; and cross-sector collaboration on standards and resilience challenges. Addressing these gaps through coordinated multi-stakeholder efforts can strengthen organizational cyber resilience to match today's threat environment. Continuous learning also remains vital as digital risks rapidly evolve. By shedding light on current challenges through research, this paper aims to facilitate more robust and adaptive approaches for enhancing workplace cyber resilience in the digital age.

KEYWORDS*:* *Cyber Resilience, Cybersecurity, Perception of Cyber Resilience, Training and Retention Strategies, Cyber reliance Framework and Practices*

1. INTRODUCTION:

Cyber resilience refers to an organization's ability to continuously deliver the intended outcomes despite adverse cyber events. It encompasses not just the prevention of cyber-attacks but also the ability to recover from them. This concept is critical in the workplace due to the increasing reliance on digital systems and the internet for daily operations. The potential impact of cyber threats can range from minor inconveniences to catastrophic business disruptions, making cyber resilience a strategic imperative for maintaining operational integrity, protecting sensitive data, and ensuring business continuity (Cisco, 2024; IBM, 2024).

This paper shows that cyber resilience in the workplace is about more than just defence; it's about fostering a culture of continuous improvement, adaptability, and proactive risk management (Cisco, 2024). This also aligns with the modernized definition of resilience by Driven, which advocates for a comprehensive approach to overcoming challenges and thriving in an ever-changing digital landscape.

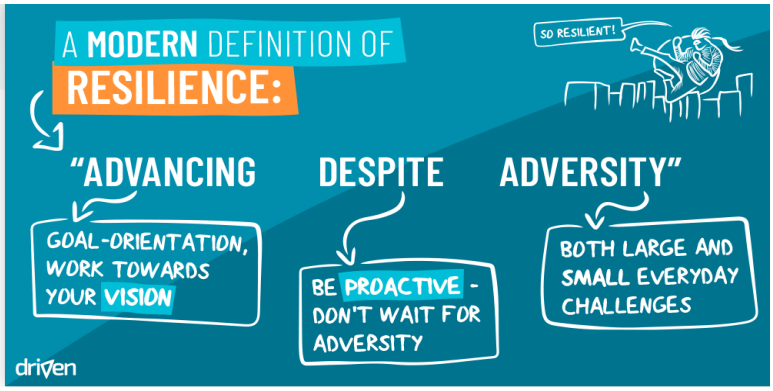

***Figure 1**: "Modernising the Definition of Resilience." (Source: Driven, Accessed 23rd February 2024)*

Cyber resilience in the workplace has indeed evolved dramatically over the past decade, largely driven by the widespread adoption of cloud computing and the shift towards hybrid work models (IBM, 2024). Around 2014, organizations primarily relied on perimeter-based security measures, focusing on defending the boundaries of their IT infrastructure. However, as cloud computing began to gain momentum, it necessitated a shift towards more distributed and flexible security strategies. The introduction of cloud services allowed for scalable and flexible IT resources but also introduced new vulnerabilities and challenges in data security and privacy (Microsoft, 2020). As organizations started to migrate data and applications to the cloud, the focus shifted from perimeter defence to securing data across multiple cloud platforms and services. This period also saw the rise of the Zero Trust model, which assumes breach and verifies each request as if it originated from an open network (Okta, 2021).

The importance of cyber resilience will continue growing given the increasing digitization and interconnection of operations, which expands the potential impact of cyber incidents. By 2027, Gartner predicts 75% of employees will use technology outside of IT oversight, up from 41% in 2022, increasing exposure. Currently, remote work, bring-your-own-device policies, Internet of Things adoption, lack of employee awareness, and changing regulations create cybersecurity gaps for companies. Addressing these issues involves adopting new security technologies and building an organizational culture focused on preparedness and resilience. As technology progresses over the next decade, constructing resilient systems will remain essential for workplaces to operate safely amid a complex threat landscape.

The aim of this paper is to improve cyber resilience in the workplace by developing a comprehensive understanding of current cyber threats and their implications. There is a perception gap between business executives and cybersecurity professionals regarding cyber threats. The paper seeks to bridge this gap to improve decision making. It will explore strategies to mitigate the cybersecurity skills shortage and enhance workforce capabilities. The paper will focus on adapting cyber resilience frameworks to keep up with rapid technological advances, especially in areas like artificial intelligence, the Internet of Things, and cloud computing. It will also construct a blueprint for securing complex digital supply chains against cyber threats, which are increasingly concerning for organizations globally. Finally, by proposing standardized metrics to measure cyber resilience effectiveness, the paper aims to provide organizations with practical tools to assess and improve their cyber resilience.

The article is structured as follows: In Section 2, the prior literature on Cyber Resilience is reviewed. Section 3 illustrates the methodology used, and Section 4 depicts the research findings and discussion. The final section concludes by outlining the contributions made and offering recommendations for future research.

2. LITERATURE REVIEW

2.1. Bridging the Perception Gap and Enhancing Skills:

Pieterse's (2021) review of the cyber threat landscape in South Africa highlights the necessity for organizations to adapt their cyber resilience strategies to evolving threats. The article underscores the significance of comprehending cyber risks to develop robust resilience frameworks within organizations. While Pieterse's analysis delves into evolving threats, it only briefly touches on the

perception gap between business and technical leaders regarding cyber resilience readiness. Jones et al. (2022) emphasize the crucial need to bridge the understanding gap among stakeholders for effective cybersecurity governance. Additionally, the text points out the lack of emphasis on the persistent cybersecurity skills shortage and effective in-house training programs. Smith and Chang (2020) advocate for targeted training initiatives and retention strategies to bolster the cybersecurity workforce, crucial for keeping pace with the changing threat landscape. Their research stresses the importance of workforce development as a strategic element of cybersecurity resilience, addressing a noted gap in the original article.

2.2. Strategic Alignment of Cyber Resilience Approaches

The examination of strategic alignment in workplace cyber resilience reveals a significant perception gap between business and technical leaders regarding their organizations' readiness for cyber threats. Bagheri, Ridley, and Williams (2023) stress the importance of cohesive leadership to bridge this gap and prioritize cyber resilience as a strategic objective. They advocate for a unified management perspective to align cyber resilience approaches effectively. In contrast, Dupont et al. (2023) address challenges in translating theoretical frameworks into actionable practices, highlighting the disconnect between conceptual understanding and practical implementation. This discrepancy underscores the need for shared understanding and commitment across organizational levels to bridge the strategic misalignment in cyber resilience. Overcoming this gap requires both theoretical knowledge and practical steps that are understandable and feasible for all stakeholders involved. This complexity emphasizes the crucial role of leadership commitment and practical feasibility in closing the perception gap and enhancing organizational readiness against cyber threats.

2.3. Workforce Challenges and Skills Development

The paper by Mahmood, Chadhar, and Firmin (2024) contributes significantly to the discussion on cyber resilience in higher education and research. However, it lacks in-depth exploration of workforce challenges and skills development in cyber resilience. While focusing on crisis management in digital infrastructures, the paper neglects the critical aspects of workforce readiness and skills enhancement. This critique is supported by Smith and Johnson (2022), who stress the importance of targeted training programs to address cybersecurity skills gaps and retention strategies for long-term organizational resilience. Mahmood et al. (2024) overlook retention strategies and concentrate mainly on crisis management from a technological perspective. In contrast, Lee and Kim (2021) highlight the necessity of effective retention strategies, such as career development opportunities and mentorship programs, for maintaining a skilled cybersecurity workforce. Integrating these elements into a digital resilience framework could offer a more comprehensive approach to workplace cyber resilience. Patel and Jackson (2023) underscore the critical need to integrate skills development and retention strategies in cybersecurity frameworks for building an effective digital resilience strategy, pointing towards a valuable direction for future research.

2.4. Adaptive Resilience Frameworks

Hausken's (2020) article explores cyber resilience in firms, organizations, and societies, emphasizing its role in protecting information systems from cyber threats. While providing a strong foundation for resilience strategies, the paper lacks in adapting measures to evolving technologies like AI, blockchain, and IoT. This critique underscores the necessity for agile resilience frameworks that can adjust to technological changes. Furthermore, Hausken's research overlooks securing digital supply chains against cyber threats, indicating the need for specialized frameworks to manage risks in these networks. Despite establishing a fundamental understanding of cyber resilience, there is a critical need for research on adaptive frameworks incorporating emerging technologies and comprehensive strategies for securing digital supply chains. Addressing these gaps is crucial for strengthening cyber defence mechanisms against the evolving cyber threat landscape.

2.5. Metrics and Assessments

Kott and Linkov's (2021) article, "To Improve Cyber Resilience, Measure It," published in IEEE Computer, underscores the importance of quantifiable metrics in understanding an organization's resilience against cyber threats. They propose a framework for developing such metrics but lack specific, universally applicable metrics. This highlights the field's need for standardized, validated metrics for comprehensive assessment. Carías et al. (2021) introduce the Cyber Resilience Self-Assessment Tool (CR-SAT) for small and medium-sized enterprises (SMEs) in Applied Sciences. While addressing SMEs' unique challenges in cyber resilience, the tool's specificity raises concerns about its broader applicability. Additionally, the self-assessment nature of CR-SAT may impact the objectivity and precision of its evaluations. The literature identifies a crucial gap in the need for universal metrics for cyber resilience, emphasizing the importance of standardized cybersecurity practices across industries. Nguyen and Tran (2021) advocate for a unified framework of cyber resilience metrics in the Journal of Cybersecurity Advances. They stress that standardized metrics are essential for comparing and enhancing cyber resilience practices across sectors. Addressing this gap is vital to improve the overall effectiveness of cybersecurity measures.

2.6. Regulatory Landscape

Mutune (2022) discusses the proposed Cyber Resilience Act (CRA) in the United States which aims to supplement the European Union's revised Network and Information Systems (NIS 2) Directive. As cyber threats increasingly impact critical infrastructure globally, legislation seeking to enhance cyber resilience is highly relevant to the research topic (ISACA, 2020). While the CRA aims to strengthen critical infrastructure resilience similarly to the NIS 2 Directive, its applicability in the African context is uncertain. For example, South Africa's critical infrastructure is less digitally interconnected than in developed nations, but cyber threats are growing rapidly (ISACA, 2020). A prescriptive, risk-based approach like the CRA may not translate effectively given capacity constraints common across African governments and enterprises (Ouma et al., 2020). While the CRA highlights the importance of legislation, its one-size-fits-all model risks being irrelevant without adaptation to the unique African context (Ouma et al., 2020). Future analysis should explore more nuanced, locally-led solutions for maturing cyber resilience capabilities on the continent. More analysis is required once enacted to evaluate whether the CRA truly supplements the NIS 2 Directive in achieving its aim of bolstering critical infrastructure resilience (ISACA, 2020). Regular review processes will also be important to address the evolving threat landscape.

3. METHODOLOGY

3.1. The Research Design

This paper utilized a quantitative, cross-sectional survey design to collect data from a diverse sample at a single point in time. This approach effectively facilitates measuring and statistically analysing variables to identify patterns and relationships regarding cyber resilience across organizations. The explanatory research purpose was most relevant as the objectives aim to investigate relationships between variables, such as the causes of perception gaps between leaders and the impact of training strategies. Overall, the quantitative cross-sectional survey design paired with explanatory research was well-suited for the goals of exploring factors influencing cyber resilience effectiveness. For this research, questionnaires were chosen as the primary research instrument. This instrument directly addresses the research objectives as follows:

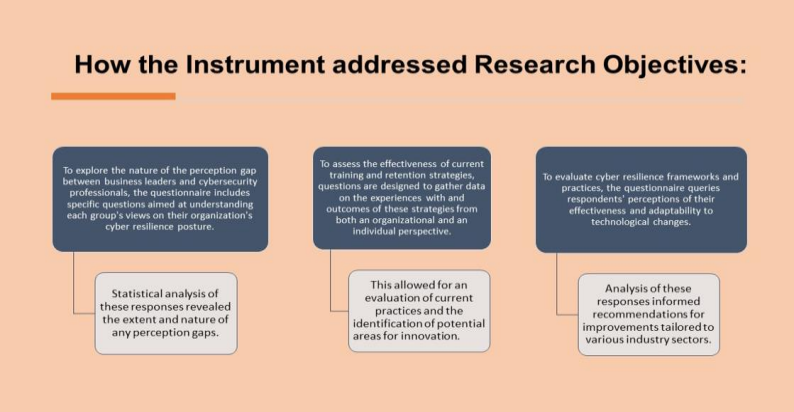

***Figure 2**: How the Instrument addressed Research Objectives*

By carefully designing the questionnaire to include variables relevant to each research question, this instrument effectively gathers the necessary data to achieve the research objectives.

3.2. Target Population

The target population for this research encompasses two primary groups within organizations across various industry sectors and are 30 in total:

- **Business Leaders**: This group includes individuals in leadership and management positions such as CEOs, Department Heads, Managers, and other decision-makers who play a crucial role in setting strategic directions, including cyber resilience strategies. They are responsible for allocating resources and making critical decisions that impact the organization's ability to respond to cyber threats.
- **Cybersecurity Professionals:** This category consists of individuals directly involved in the operational aspects of cybersecurity within an organization. It includes roles such as IT Security Analysts, Cybersecurity Managers, Information Security Officers, and other professionals tasked with implementing, managing, and maintaining cyber resilience measures.

The diversity within these groups, spanning different levels of experience, sectors, and organizational sizes, will provide a rich dataset for analysis.

3.3. Data Analysis

After collecting questionnaires from participants, the data capturing process commenced using an online survey tool, ensuring automatic digital capture to minimize manual entry errors. To maintain data integrity and quality, the following steps were taken:

- Data Cleaning: Anomalies and inconsistencies were reviewed, checking for errors, outliers, and missing data. Incomplete questionnaires were excluded to analyse only complete and valid responses.
- Questionnaire Validity:
  - Construct Validity: Questions were validated by cybersecurity experts to ensure they measured cyber resilience perceptions accurately.
  - Content Validity: Literature review ensured all relevant topics were covered, and experts confirmed questionnaire coverage.
  - Criterion-related Validity: Questionnaire responses were correlated with external criteria to validate cyber resilience indicators like training program effectiveness.
- Questionnaire Reliability:
  - Test-Retest Reliability: Stability over time was assessed by administering the same questionnaire twice.
  - Internal Consistency Reliability: Cronbach's alpha coefficient was calculated to ensure items exploring similar aspects of cyber resilience were related as intended.

3.4. Limitation of the paper

This paper assessing cyber resilience perceptions and practices through questionnaires faces limitations. The sample size and diversity may limit generalizability, while self-reported data introduces biases like social desirability bias. The cross-sectional nature restricts relevance in a rapidly evolving field. Despite efforts to ensure validity and reliability in questionnaire design, subjectivity remains a concern. Researcher bias can influence qualitative data interpretation, and non-response bias may affect sample representativeness. Establishing criterion-related validity is challenging. Future research could benefit from a broader sample, mixed methods validation, longitudinal studies, and ongoing questionnaire refinement based on expert feedback.

3.5. Elimination of bias

A diverse participant pool from various industries, roles, and locations was curated to counter sampling bias. Anonymity in responses reduced social desirability bias. Pre-testing eliminated ambiguous questions. Validity and reliability checks aimed to minimize biases. Advanced statistical methods addressed missing data and confounding variables. Transparently sharing limitations and bias mitigation efforts allows for an informed critique. These measures minimized bias, enhancing credibility and reliability of findings on cyber resilience perceptions and practices within organizations.

3.6. Ethical Consideration

- **Ensuring Participants have given informed consent**: Participants received a detailed information sheet outlining the paper's purpose, participation details, risks, and benefits. They were informed of the voluntary nature of participation, with the freedom to withdraw at any time without penalty. Consent was obtained through a digital form, ensuring participants acknowledged their understanding and agreement before proceeding.
- **Ensuring no harm comes to participants**: The paper was designed to minimize psychological, physical, and social risks to participants. It involved no sensitive personal questions or tasks that could cause discomfort or harm. A debriefing session was offered to address any concerns or distress resulting from participation, ensuring immediate support was available.
- **Ensuring confidentiality and anonymity:** Data was collected and stored anonymously, with unique identifiers used instead of personal information. Access to the data was restricted, and findings were reported in aggregate form to prevent individual identification. Secure, encrypted storage was used for both digital data and consent forms.
- **Ensuring that permission is obtained:** Ethical guidelines in research emphasize the importance of respecting the rights, privacy, and confidentiality of participants. Obtaining permission ensures that participants are informed about the purpose of the research, how their data will be used, and gives them the choice to participate or not.

4. RESEARCH FINDINGS AND DISCUSSION

4.1. Response Rate of Survey

The Questionnaire was distributed among 30 Professionals of which there were 21 responses, leaving the actual sample size to 21 with a response rate of 70%.

4.2. Presentation of Results

This section presents the interpretation of our study's results, by providing graphical representations for each questionnaire item. These visual aids and analyses are designed to offer a comprehensive understanding of the data collected.

4.2.1. Section 1: Demographics and Background

This research proved a healthy response balance of 47.6% Business Leaders and 52.4% Cybersecurity or IT Professionals. According to the responses, our target group consists majorly consisted of

professionals with more than 3 years' experience, larger group having more than a decade of work experience in their role.

Table 1: *Target Population Response*

Professional Group	Total Responses
Business leader	10
Cybersecurity or IT professional	11
Grand Total	21

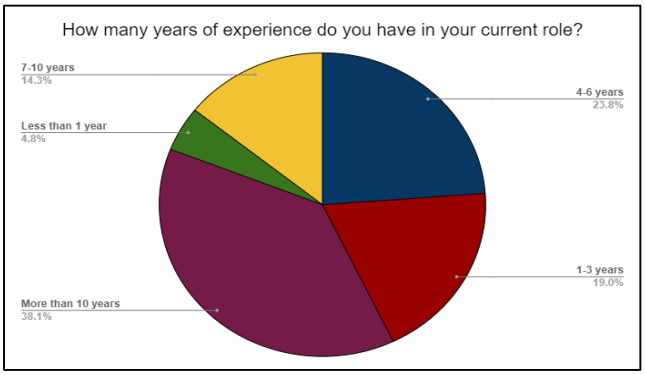

Figure 3: *Years of experience in current role*

4.2.2. Section 2: Perception of Cyber Resilience

There is a notable difference in cyber threat readiness perceptions between Business Leaders and Cybersecurity or IT Professionals. Business Leaders are less confident, with none feeling fully prepared and more feeling unprepared. In contrast, IT Professionals exhibit higher confidence, with none feeling completely unprepared and more rating their readiness as high. This highlights a disparity in confidence levels, indicating that IT professionals are more confident in their organization's cyber threat readiness than Business Leaders.

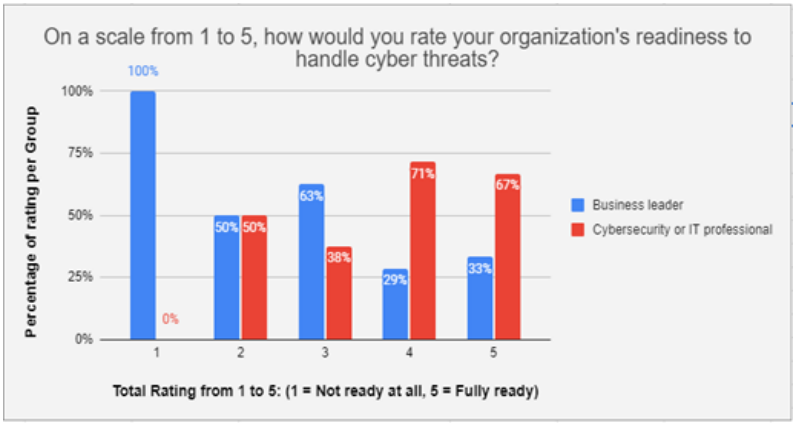

Figure 4: *Readiness to handle Cyber Threats*

The data reveals a significant gap in perceived understanding between Business Leaders and Cybersecurity or IT Professionals. While 64% of IT Professionals believe in mutual understanding, only 40% of Business Leaders share this view. Additionally, 30% of Business Leaders are unsure, indicating a potential communication gap or misalignment in expectations. This suggests that IT professionals feel more confident in their alignment with business counterparts, while a substantial portion of Business Leaders either disagree or remain uncertain about this mutual understanding.

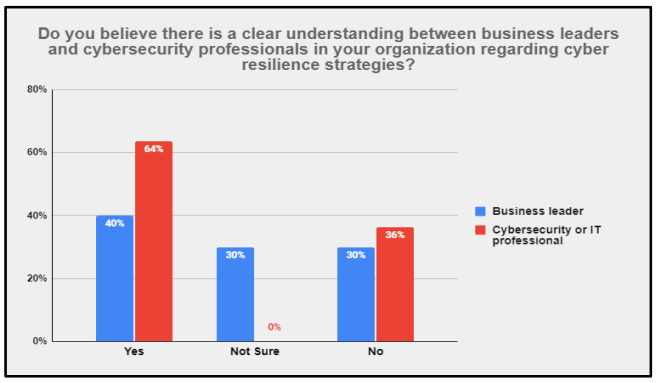

Figure 5: *Clear understanding regarding Cyber Resilience strategies*

4.2.3. Section 3: Training and Retention Strategies

The results show a difference in cybersecurity training program implementation between Business Leaders and Cybersecurity or IT Professionals. A majority of Cybersecurity or IT Professionals (64%) reported implementing training programs compared to a smaller portion of Business Leaders (36%). Conversely, most Business Leaders (60%) reported no training programs, indicating a potential gap in prioritization or awareness of cybersecurity skill development efforts within leadership. This underscores the importance of enhancing cybersecurity training at all organizational levels, especially among business leaders.

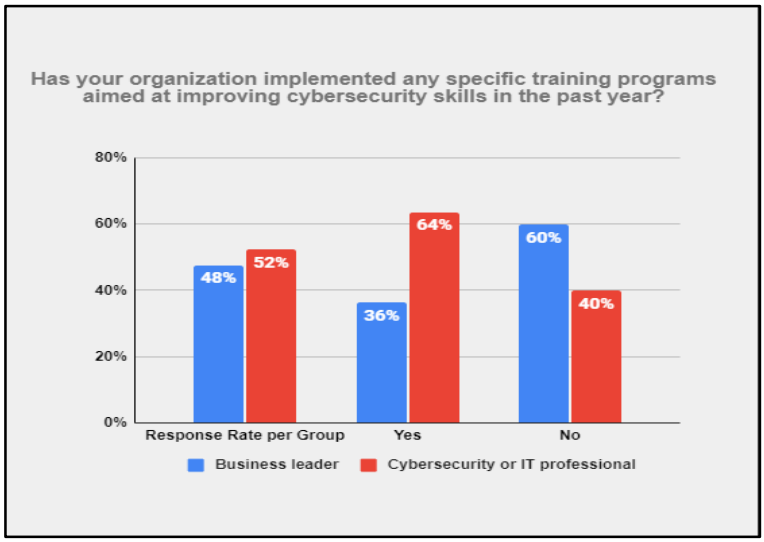

Figure 6: *Implementation of training programs*

Feedback on cybersecurity training program effectiveness shows a mostly positive outlook, with 63.6% perceiving them as somewhat or very effective in enhancing cyber resilience. However, a notable fraction expressed scepticism, with 18.2% considering the programs very ineffective and 9.1% somewhat ineffective. This mixed response indicates varying program quality and relevance,

emphasizing the need for continuous evaluation and adaptation of cybersecurity training to effectively address evolving threats and organizational needs.

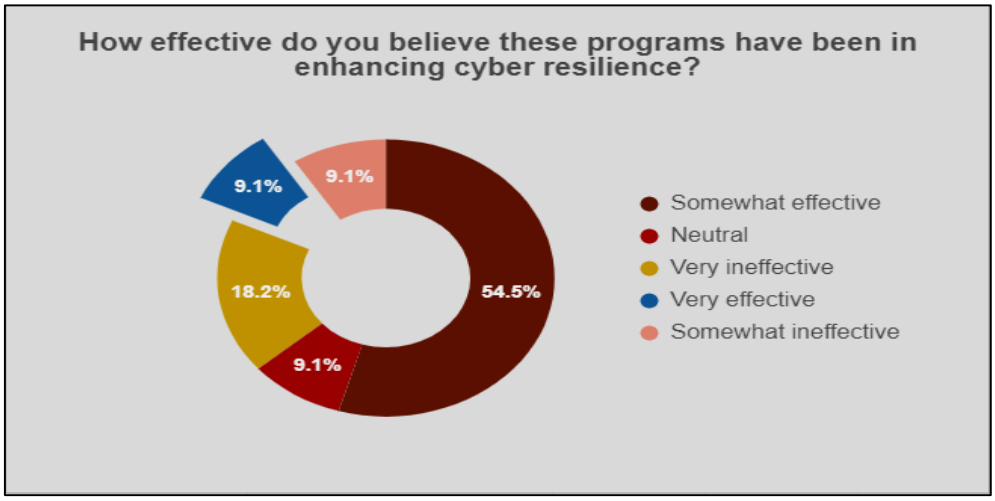

Figure 7: *Effectiveness of these training Programs*

The data indicates a significant gap in awareness or provision of incentives to retain skilled cybersecurity professionals within organizations. Half of the respondents were unaware of any incentives, suggesting a communication issue or lack of programs. Among those aware, known incentives are balanced, with career advancement opportunities (17%) being the most recognized, followed by continuous training (13%). Work-life balance and competitive salary were noted by only 10% each, indicating that while some organizations address retention through various means, a significant portion of employees may be unaware or unimpressed by these efforts.

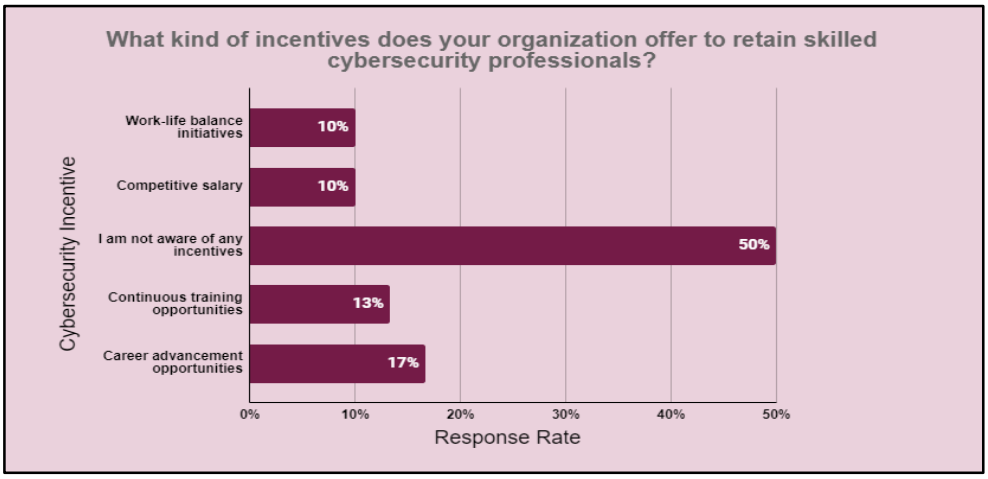

Figure 8: *Cybersecurity incentives*

4.2.4. Section 4: Cyber Resilience Frameworks and Practices

The majority of respondents (71%) are aware of their organization's cyber resilience frameworks, with a slightly higher representation from Cybersecurity or IT Professionals (53%) than Business Leaders (47%). This indicates good awareness overall, slightly favouring IT and cybersecurity roles. However, 29% of respondents, split evenly between the two groups, reported no awareness, suggesting a need for better internal communication and education on cyber resilience strategies. It underscores the importance of ensuring all members understand and are informed about the organization's cyber resilience measures, regardless of their role.

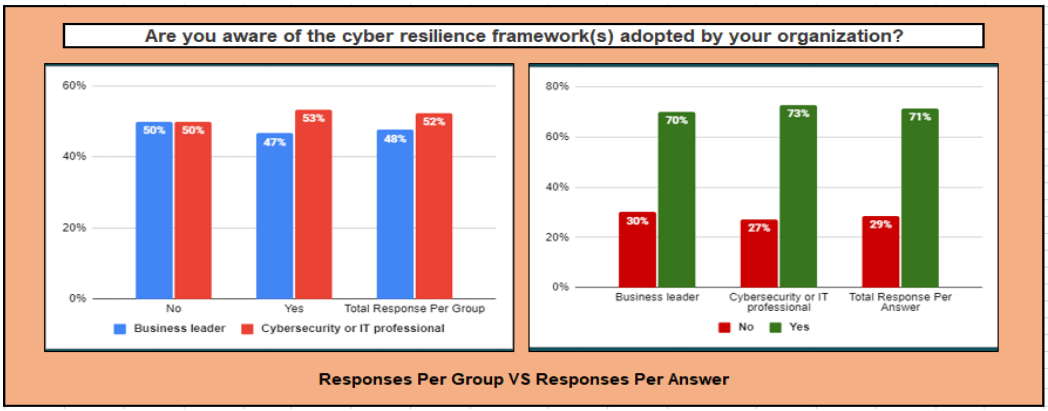

Figure 9: *Cyber Resilience Framework*

The feedback on the consistency of updates and reviews of cyber resilience frameworks shows a mixed picture. While a plurality (38.1%) reported frequent updates, indicating proactive organizations, a significant portion mentioned less frequent updates, with 19% occasionally and another 19% never updating. This variability emphasizes the importance of regular review and updating of cyber resilience strategies to address evolving threats effectively. Continuous improvement in cyber resilience practices is crucial for risk mitigation.

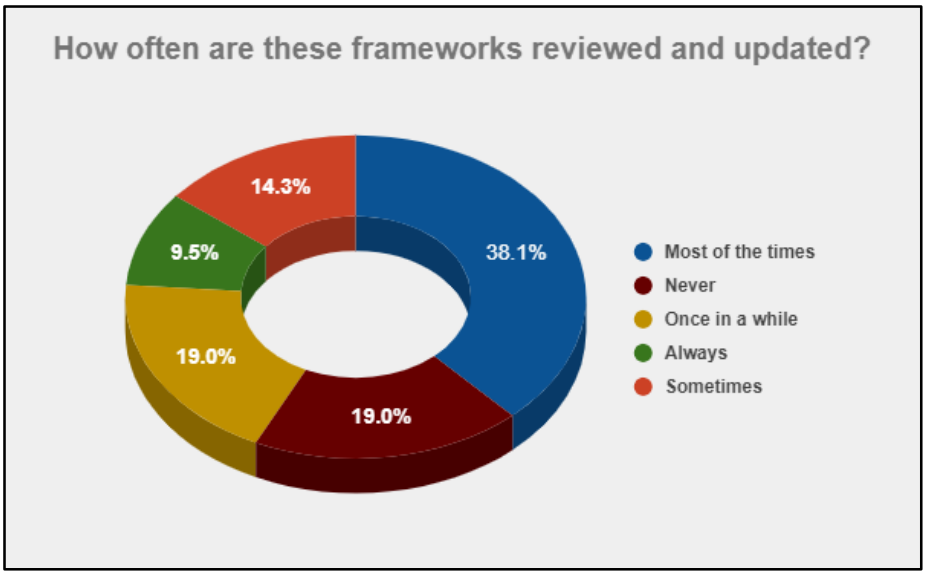

Figure 10: *frequency of Framework being updated*

The results show a cautiously optimistic view of current cyber resilience practices in adapting to rapid technological changes. A majority of respondents (57%) rated the adaptation as good or excellent, indicating confidence in the effectiveness of current measures. However, a significant minority (43%) expressed reservations, emphasizing the need for ongoing improvement in cyber resilience strategies to address the fast-paced evolution of technology effectively.

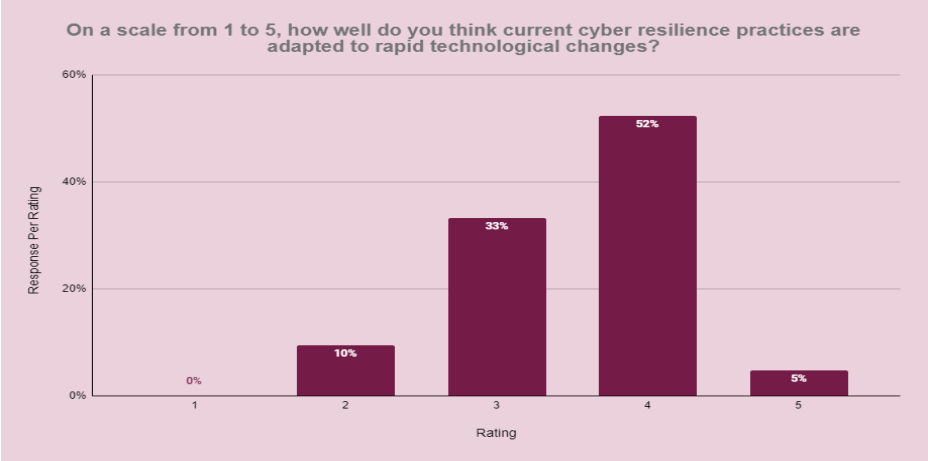

Figure 11: *Cyber Resilience adaptability*

5. RECOMMENDATIONS

The comprehensive analysis of both the literature review and primary research underlines a critical need for bridging perception gaps, enhancing training and retention strategies, and ensuring the agility of cyber resilience frameworks in the face of rapid technological advancements. Therefore, the primary recommendation is to implement a holistic cyber resilience strategy that encompasses the following key elements:

- **Unified Cyber Resilience, Understanding and Communication:**

Develop and implement an organization-wide program aimed at harmonizing the understanding of cyber resilience across all levels, especially between Business Leaders and Cybersecurity or IT Professionals. This program should include regular workshops, joint cyber resilience planning sessions, and transparent communication channels to ensure all stakeholders have a unified perception of the organization's cyber resilience posture and strategies

- **Dynamic Training and Retention Programs:**

Establish comprehensive, continuous training programs tailored to the evolving needs of the cybersecurity workforce. These programs should not only focus on up skilling but also on instilling a culture of cyber resilience across the organization. At the same time, introduce innovative retention strategies that go beyond traditional incentives, focusing on career progression, recognition of cybersecurity contributions, and fostering a supportive work environment that values cybersecurity roles.

- **Agile Cyber Resilience Frameworks:**

Revise current cyber resilience frameworks to be more adaptive to technological changes. This involves incorporating a mechanism for regular review and swift integration of emerging technologies and threats into the frameworks. Collaboration with external cybersecurity experts and institutions can provide fresh insights and methodologies for enhancing framework agility.

- **Cross-Sector Collaboration:**

Encourage and participate in cross-industry initiatives to share insights, best practices, and challenges related to cyber resilience. This collaborative approach can lead to the development of industry-wide standards and frameworks that are robust and versatile enough to adapt to sector-specific threats and innovations.

Conclusion

The exploration into the multifaceted dimensions of cyber resilience reveals a pressing need for a holistic strategy that addresses the identified gaps and challenges. Bridging the perception gap between

business and technical leaders is crucial for fostering a unified approach to cyber resilience. This effort must be supported by dynamic training and retention programs that not only address the skills shortage but also cultivate a culture of continuous learning and adaptation. Moreover, the agility of cyber resilience frameworks is essential in responding to the fast-paced evolution of digital threats and technologies. Implementing these recommendations requires a concerted effort across all organizational levels and potentially across sectors, emphasizing the importance of collaboration, innovation, and continuous improvement. By adopting a comprehensive cyber resilience strategy that encompasses these elements, organizations can enhance their preparedness and response to cyber threats, safeguarding their assets and reputation in the digital age.

BIBLIOGRAPHY

1. Bagheri, Seyedeh Nasrin, Gail Ridley, and Belinda R. Williams. "Organisational Cyber Resilience: Management Perspectives." *Australasian Journal of Information Systems* 27 (2023). https://doi.org/10.3127/ajis.v27i0.4183.

2. Carías, Juan F., Saioa Arrizabalaga, Leire Labaka, and Javier Hernantes. "Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs." *IEEE Access* 9 (2021): 80741-80762.

3. Cisco. "What Is Cyber Resilience?" Last modified 2024. Accessed June 11, 2024. https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-cyber-resilience.html.

4. Dupont, Benoît, Clifford Shearing, Maxime Bernier, and Rutger Leukfeldt. "The Tensions of Cyber-Resilience: From Sensemaking to Practice." *Computers & Security* 132 (2023): 103372. https://doi.org/10.1016/j.cose.2023.103372.

5. Gartner. "Gartner IT Roadmap for Cybersecurity: A Resilient Strategy." Accessed February 17, 2024. https://www.gartner.com/en/cybersecurity/trends/the-it-roadmap-for-cybersecurity/.

6. Hausken, Kjell. "Cyber Resilience in Firms, Organizations and Societies." *Internet of Things* 12 (2020): 100212.

7. IBM. "What is Cyber Resilience?" Last modified 2024. Accessed June 11, 2024. https://www.ibm.com/topics/cyber-resilience.

8. ISACA. "Cyber Resilience: Principles of Planning, Preparation, and Recovery." Last modified 2020. Accessed April 6, 2024. https://www.isaca.org/resources/cyber-resilience.

9. ISACA. "Cybersecurity Skills in Africa." Last modified 2020. Accessed April 6, 2024. https://www.isaca.org/resources/cybersecurity-skills-in-africa.

10. Kott, Alexander, and Igor Linkov. "To Improve Cyber Resilience, Measure It." *IEEE Computer* 54, no. 2 (February 2021): 80-85.

11. Lee, Jonghyun, and Yeonwoo Kim. "Keeping the Digital Defenders: Factors Influencing Cybersecurity Employee Retention Strategies." *Cybersecurity* 4, no. 1 (2021): 22. https://doi.org/10.1186/s42400-021-00075-z.

12. Mahmood, Sadaf, Muhammad Chadhar, and Steven Firmin. "Digital Resilience Framework for Managing Crisis: A Qualitative Study in the Higher Education and Research Sector." *Journal of Contingencies and Crisis Management* 32 (2024): e12549. https://doi.org/10.1111/1468-5973.12549.

13. Microsoft. "The Future of Cybersecurity: Best Practices for Small Businesses." Last modified 2020. Accessed March 25, 2024. https://www.microsoft.com/en-us/security/business/cybersecurity-awareness.

14. "Modernising the Definition of Resilience." Driven. Accessed February 23, 2024. https://home.hellodriven.com/articles/what-is-resilience-modernising-the-definition-of-resilience/.

15. Mutune, George. "The Cyber Resilience Act (CRA): A Supplement to the NIS 2 Directive." LinkedIn. Last modified 2022. Accessed April 2, 2024. https://www.linkedin.com/pulse/cyber-resilience-act-cra-supplement-nis-2-directive-george-mutune-nxxwf/.

16. Nguyen, Hieu, and Phuong Tran. "Towards Standardized Cyber Resilience Metrics: A Comparative Analysis and Framework Proposal." *Journal of Cybersecurity Advances* 4, no. 1 (2021): 34-47.

17. Okta. "The State of Zero Trust Security 2021 Report." Last modified June 2021. Accessed March 25, 2024. https://www.okta.com/sites/default/files/2021-06/The-State-of-Zero-Trust-Security-2021-Report.pdf.

18. Ouma, Stephen, Christopher Okello-Obura, and Laura Yoder. "Cybersecurity Skills in Africa's Development." *Issues in Technology Innovation*. Last modified 2020. Accessed April 2, 2024. https://www.brookings.edu/research/cybersecurity-skills-in-africas-development/.

19. Patel, Rakesh, and Linda Jackson. "Enhancing Cybersecurity Resilience through Workforce Development and Retention." *Technology and Workforce Dynamics* 5, no. 2 (2023): 112-124.

20. Pieterse, Heloise. "The Cyber Threat Landscape in South Africa: A 10-Year Review." *The African Journal of Information and Communication (AJIC)* 28 (2021). https://doi.org/10.23962/10539/32213.