Vol.4, No.5, Page 2042- 2048, 2026 https://doi.org/10.59628/jast.v4i5.2469 ISSN 2958-9568 JAST

SUN PUBLISHER

مجلة جامعة صنعاء للعلوم التطبيقية والتكنولوجيا

Sana'a University Journal of Applied Sciences and Technology

https://journals.su.edu.ye/index.php/jast/

Enhancing Cybersecurity in Yemeni Universities: A Socio-Technical Model

Maged Saeed Saeed Ali [1]*, Khalil Saeed Al-Wagih[2], Fawaz Mahioub Mohammed Mokbal Alghfari[1] and Abdulrahman Ali Abdullah AL-Akwaa[1]

[1]**Department of Computer Science, Faculty of Computer and Information Technology, Sana'a University, Sana'a, Yemen,**
[2]**Department of Computer Science, Faculty of Computer and Information Technology, Dhamar University, Dhamar, Yemen**

*Corresponding author: Maged.Ali@su.edu.ye

Abstract

The digital transformation of higher education institutions in conflict-affected regions presents acute cybersecurity challenges compounded by resource constraints. This study responds to the need for context-specific frameworks by diagnosing the cybersecurity posture of Yemeni universities and developing an empirically-grounded enhancement model. Employing a descriptive-analytical quantitative design, data were collected via a structured questionnaire from 93 key stakeholders across five universities in Sana'a, measuring Technical Practices, Governance, Awareness & Capacity Building, and Model Adoption Readiness. Statistical analysis, enhanced with effect size measures (η^2) and checks for common method bias, revealed moderate implementation of basic controls but critical deficiencies in proactive measures and governance. Awareness & Capacity Building was the strongest predictor of readiness ($r = 0.85$, $p < 0.01$). A two-way ANOVA showed academic qualification (PhD) had a significant, moderate effect on readiness ($\eta^2 = 0.08$, $p = 0.024$), while years of service had no significant effect. Grounded in Socio-Technical Systems (STS) Theory, the study proposes a Cybersecurity Enhancement Model (CEM) comprising five synergistic domains: Inclusive Governance, Technical Controls, Human-Centered Capacity Building, Risk Communication, and Continuous Improvement, operationalized through a PDCA cycle. A functional Flask-based web application (CEM App) is presented to facilitate implementation. This research contributes a pragmatic, validated framework tailored for resource-constrained environments, bridging the gap between international standards and on-the-ground realities in conflict-affected higher education.

Article Info

Keywords:
Cybersecurity, Higher Education, Integrative Framework, Institutional Readiness, Socio-Technical Systems, Capacity Building, Yemen, Biometric Authentication.

Article History:
Received: 03-November-2025,
Revised: 11-February-2026,
Accepted: 29-April-2026,
Published: 28 May 2026.

1. INTRODUCTION

The pervasive digitization of higher education has intrinsically linked academic missions to vulnerable cyber-physical infrastructures, making universities high-value targets for espionage, data theft, and disruptive ransomware attacks [1, 2]. This global vulnerability is critically amplified in developing nations facing complex emergencies, such as Yemen, where a confluence of chronic underfunding, scarce technical expertise, and deteriorating infrastructure creates a uniquely challenging threat landscape [3, 4]. In such contexts, prevailing approaches that prioritize technical controls in isolation are insufficient. A paradigm shift is required, reconceptualizing cybersecurity as a**socio-technical system** where technological measures are inextricably linked to and dependent upon robust governance and human capabilities [5, 6].

While international standards (e.g., NIST Cybersecurity Framework [CSF], ISO/IEC 27001) provide comprehensive guidelines [7, 8], their direct application in severely resource-constrained environments often fails due to a lack of contextual adaptation [9]. A significant literature gap exists in empirically derived models that are both theoretically sound and pragmatically feasible for institutions operating under duress [10]. This study directly addresses this issue. The objectives of this study are threefold: (1) to conduct a diagnostic assessment of the

current cybersecurity landscape in Yemeni universities using robust empirical methods; (2) to evaluate the institutional readiness for a structured enhancement model while rigorously testing the influence of key demographic factors; and (3) to design, propose, and partially implement a practical, integrative Cybersecurity Enhancement Model (CEM). The research is guided by the central question:**What is the state of cybersecurity readiness in Yemeni universities, and how do technical, governance, and human factors predict the capacity to adopt a holistic enhancement framework?** By answering this question, this study provides a validated roadmap for sustainable improvement.

2. RELATED WORK

2.1. Cybersecurity in Higher Education: Global and Regional Perspectives

Cybersecurity challenges facing higher education institutions (HEIs) have garnered increasing global scholarly attention. Research highlights their attractiveness as targets because of their open networks, valuable research data, and often decentralized IT governance [1, 2]. Frameworks and studies from developed contexts emphasize comprehensive approaches that integrate risk management, governance (often aligned with standards such as ISO/IEC 27001 and NIST CSF [7, 8]), and continuous awareness training [11, 12]. However, as noted by Catota et al. [4] and Alshaikh [9], the direct application of these resource-intensive models in developing regions is problematic. Studies in contexts such as Saudi Arabia [9] and Ecuador [4] begin to address this, pointing to challenges of funding, expertise, and infrastructure, but often remain focused on technical or educational silos rather than integrated institutional reform.

2.2. The Socio-Technical Paradigm in Cybersecurity

A growing strand of literature argues for viewing cybersecurity through a socio-technical lens. Grounded in the foundational work of Trist and Bamforth [13], this paradigm posits that effective security emerges from the joint optimization of social and technical subsystems. Von Solms and Van Niekerk [5] were instrumental in shifting the discourse from "information security" to "cybersecurity," emphasizing broader organizational and human factors. Subsequent work, such as that by Malatji et al. [14] and Zoto et al. [15], explicitly applies STS principles to design cybersecurity frameworks, arguing that technical controls fail without congruent social structures, processes, and culture. This body of work provides a theoretical justification for moving beyond checklists to holistic models.

2.3. The Contextual Research Gap in Conflict-Affected States

Despite these advances, a critical gap remains. There is a paucity of empirical research designing and validating cybersecurity frameworks for HEIs in**conflict-affected and severely resource-constrained environments**like Yemen. Al-Hadhrami et al. [3] and Humied [10] point to the acute nature of the challenge in the Yemeni context but stop short of proposing a holistic, empirically tested operational model. Most existing models are either conceptual, adapted from Western contexts without validation, or focus solely on technical or educational aspects of the problem. This study fills this gap by deriving an integrative model from primary data collected*in situ*, ensuring that it addresses the unique socio-technical realities—such as fluctuating resources, institutional fragmentation, and heightened human factor vulnerabilities—of universities in such environments.

3. THEORETICAL FRAMEWORK: SOCIO-TECHNICAL SYSTEMS (STS) THEORY.

3.1. STS as the Foundational Lens

This research is explicitly grounded in Socio-Technical Systems (STS) Theory [13]. The core STS premise is that organizational performance and resilience are optimized when social (people, culture, governance, and processes) and technical (tools, infrastructure, and controls) subsystems are designed interdependently, not in isolation [16]. This represents a shift from a reductionist, technology-centric view to a holistic and systemic view.

3.2. Application to Cybersecurity Enhancement

For cybersecurity, the STS lens mandates a move beyond siloed technical solutions. It frames cybersecurity resilience as an*emergent property* of a well-designed socio-technical system. This implies:

Joint Optimization: Investments in technology must be matched by investments in governance capability and human competency. A sophisticated firewall is ineffective without policies governing its rules and administrators trained to manage them.

Interdependence: The effectiveness of any subsystem is contingent on the others. For example, the success of an awareness program (social) depends on technical channels for delivery and measurement, whereas the value of intrusion detection logs (technical) depends on social processes for analysis and response.

Adaptive Design: The system must be designed for local constraints and affordances, not merely imported as a "best practice" [14, 15]. This means prioritizing scalable, low-cost human and process innovations, alongside appropriate technology.

Table 1. Sample Distribution by Institution and Role

University	Type	Faculty	Admin Staff	Students	Total
Sana'a University	Public	46	4	14	64
21 September University	Public	12	2	8	22
University of Science & Tech.	Private	15	3	13	31
Al-Takhassusi University	Private	11	2	9	22
Al-Mustaqbal University	Private	7	1	7	15
Total (Sampling Frame)		91	12	51	154

The proposed Cybersecurity Enhancement Model (CEM) is a direct operationalization of these principles, structuring interventions across five interdependent domains that mirror core socio-technical components.

4. RESEARCH METHODOLOGY

4.1. Design and Sampling Rationale

A descriptive-analytical quantitative design was selected to objectively characterize current practices, test relationships between variables, and provide a robust empirical foundation for model development. The target population included faculty, senior administrative staff, and advanced (final-year) cybersecurity students from five universities in Sana'a (two public and three private). This triangulation of perspectives—from policymakers and implementers to theoretically informed students—ensured a comprehensive view of the institutional landscape. Purposive sampling was employed to strategically capture the diversity of key informants. From an initial sampling frame of 154 eligible individuals, 110 questionnaires were distributed. Nine questionnaires were excluded due to incomplete data (>20% of questions were blank), yielding 93 valid responses—an exceptionally high response rate of 84.55% that strengthens the reliability of the findings. The distribution is shown in Table 1.

4.2. Instrument Development and Validation

A structured questionnaire was developed with four sections using a 5-point Likert scale (1=Strongly Disagree to 5=Strongly Agree):

1. **Demographics.**
2. **Cybersecurity Practices (25 items):** It covers asset management, access control, monitoring, incident response, and proactive security (e.g., "Penetration tests are conducted regularly").
3. **Governance & Awareness (25 items):** Split into Governance and Policy (12 items, e.g., "There is a dedicated budget for cybersecurity initiatives") and Awareness & Capacity Building (13 items, e.g., "Staff receive regular cybersecurity training relevant to their role").
4. **Model Readiness (15 items):** Assessing willingness, perceived resource availability, leadership support, and feasibility of adopting a new framework (e.g., "Leadership at my university would support implementing a comprehensive cybersecurity model").

Table 2. Reliability Analysis of Measurement Scales (n=93)

Dimension	No. of Items	Cronbach's Alpha (α)	Interpretation
Cybersecurity Practices	25	0.91	Excellent
Governance and Policy	12	0.88	Good
Awareness & Capacity Building	13	0.86	Good
Model Readiness	15	0.89	Good

Content and face validity were established through an iterative review by a panel of five experts in cybersecurity and higher-education management. A pilot test (n=15) confirmed the clarity and appropriateness of the questionnaire. Reliability was statistically confirmed using Cronbach's alpha, with all composite scales demonstrating excellent internal consistency (> 0.85), as shown in Table 2.

4.3. Data Analysis and Statistical Enhancements

All analyses were performed using SPSS v27. The planned analysis was expanded in direct response to the methodological feedback to enhance rigor.

1. **Descriptive Statistics:** To profile the implementation level of each dimension.
2. **Pearson Correlation:** To examine bivariate relationships between the main study variables.
3. **Two-Way ANOVA:** To test for differences in Model Readiness scores based on *Years of Service* (categorized as <5, 5-10, 11-15, >15) and*Academic Qualifi-*

Table 3. Descriptive Statistics for Key Cybersecurity Practice Items (n=93)

Statement	Mean (M)	Std. Deviation (SD)	Interpretation
A dedicated cybersecurity team exists.	3.44	0.97	Moderate Implementation
Business continuity plans exist.	2.34	1.19	Low Implementation
Red-team simulations are conducted.	2.29	1.20	Low Implementation
Penetration tests are conducted.	2.53	1.15	Low Implementation
A formal incident response policy exists.	2.46	1.13	Low Implementation

cation (Bachelor's, Master's, and PhD). **Effect sizes (η^2 - Eta Squared)** were calculated for all ANOVA effects to distinguish statistical significance from practical significance [17].

4. **Common Method Bias Assessment:**Acknowledging the use of self-reported data,**Harman's Single-Factor Test** was conducted post-hoc using Principal Axis Factoring. The unrotated solution revealed that the first factor accounted for**31.2%**of the total variance, which is well below the 50% threshold, indicating that common method bias is unlikely to be a serious contaminant in this dataset [18].

5. RESULTS AND ANALYSIS

5.1. Diagnostic Assessment of Current Posture

Descriptive analysis painted a concerning yet actionable picture. Foundational technical controls were moderately present (e.g., existence of a dedicated team, M=3.44). However, as detailed in Table 3, critical proactive and strategic measures were severely underdeveloped, indicating a reactive rather than resilient security stance.

5.2. Governance and Human Factor Maturity

Governance maturity was low (Aggregate $M \approx 2.63$), characterized by absent steering committees ($M = 2.48$) and minimal strategic budgeting ($M = 2.39$). Awareness and capacity efforts were moderately recognized (Aggregate $M \approx 2.65$) but lacked systematic evaluation ($M = 2.37$ for training effectiveness), indicating that programs were not data-driven or outcome-focused.

5.3. Readiness for Holistic Model Adoption

Overall readiness for adopting the proposed CEM was moderate to low (Aggregate M = 2.68). Readiness was highest for process-oriented improvements, such as the PDCA cycle (M=2.88), and lowest for initiatives requiring sustained cultural engagement, such as risk communication newsletters (M=2.47) and establishing a security champions network (M=2.54).

5.4. Interrelationships between Constructs

Pearson correlation analysis, presented in Table 4, revealed strong, statistically significant positive relationships ($p < .01$) among all core dimensions. Notably,**Awareness & Capacity Building shared the strongest association with Model Readiness (r = .85)**, powerfully emphasizing that readiness is fundamentally linked to human and organizational development.

5.5. Influence of Demographic Variables

A two-way ANOVA was conducted to assess the effects of Demographic Variables A model readiness scores. The complete results, including the requested effect size measures, are presented in Table 5.

*Post-hoc*comparisons (LSD) for Academic Qualification revealed that participants holding a PhD (M = 3.12, SD = 0.89) reported significantly higher readiness scores than those with a Master's (M = 2.65, SD = 0.91, p = .018) or a Bachelor's degree (M = 2.58, SD = 0.87, p = .009). The effect size (η^2 = 0.08) indicates **moderate practical significance**, suggesting that advanced academic expertise is a meaningful asset in championing cybersecurity change. The non-significant result for Years of Service (η^2 = 0.02) indicates that institutional tenure alone does not influence readiness perceptions.

6. THE CYBERSECURITY ENHANCEMENT MODEL (CEM): AN STS-BASED FRAMEWORK

Synthesizing the empirical findings within the STS theoretical lens, we propose a Cybersecurity Enhancement Model (CEM). The CEM integrates five interdependent domains within a continuous plan-do-check-act (PDCA) cycle, creating a dynamic system for sustainable improvement, as illustrated in Figure 1.

Table 4. Pearson Correlation Matrix between Study Variables

Variable	1. Practices	2. Governance	3. Awareness	4. Readiness
1. Practices	1			
2. Governance	.78**	1		
3. Awareness	.72**	.81**	1	
4. Readiness	.69**	.75**	.85**	1
** p < .01 (2-tailed)				

Table 5. Two-Way ANOVA Results for Model Readiness Scores with Effect Sizes

Source	S-Sq	df	M-S	F	p-value	η^2 **(Effect Size)**	Interpretation
Academic Qualification	45.21	2	22.60	3.91	**0.024**	**0.08**	Moderate Effect
Years of Service	8.32	3	2.77	0.72	0.49	0.02	Negligible Effect
Qualification * Service	21.45	6	3.58	1.12	0.35	0.04	Negligible Effect
Error	512.33	87	5.89				

S-Sq=Sum of Squares, MS=Mean Square

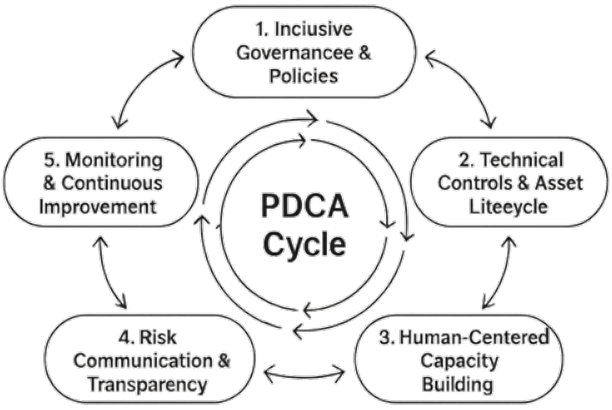

Figure 1. The Cybersecurity Enhancement Model (CEM) Framework

6.1. Model Domains

1. **Inclusive Governance & Policies:** Establishes strategic direction via a cross-functional Cybersecurity Steering Committee with representation from academia, administration, and IT. This domain mandates participatory policy co-creation workshops and transparent, risk-informed budgeting, directly addressing the governance gaps identified in this study.
2. **Technical Controls and Asset Lifecycle:** Promotes a risk-based approach, prioritizing foundational hygiene (e.g., asset inventory and patch management) while planning for advanced controls. It integrates security into the procurement and system development lifecycles, ensuring sustainability.
3. **Human-Centered Capacity Building:**Moves beyond one-size-fits-all training. It develops tiered, role-based learning paths (e.g., for researchers, finance staff), a "Security Champions" peer-mentoring network, and incentive structures to reward secure behaviors, directly leveraging the finding that awareness is the key readiness predictor.
4. **Risk Communication & Transparency:**Builds organizational trust through regular "Risk Capsule" newsletters, an anonymous incident-reporting portal with a guaranteed feedback loop, and interactive dashboards showing security metrics. This addresses the low readiness for such communicative actions.
5. **Monitoring & Continuous Improvement:** Embeds evidence-based refinement using the PDCA cycle. It involves annual maturity assessments against adapted standards (e.g., a simplified NIST CSF) and the production of an annual Cybersecurity Transparency Report to maintain accountability, and drive progress.

7. OPERATIONALIZATION: THE CEM WEB APPLICATION

To transition the CEM from a conceptual framework to an actionable management tool, a functional web application (CEM App) was developed using Python's Flask framework, following an MVC pattern. The core database schema, designed to encapsulate the model's logic, is shown in the Entity-Relationship Diagram (ERD) in Figure 2.

The application's "CEM Engine" automates key processes: it hierarchically calculates domain and overall Organizational Readiness Index (ORI) scores based

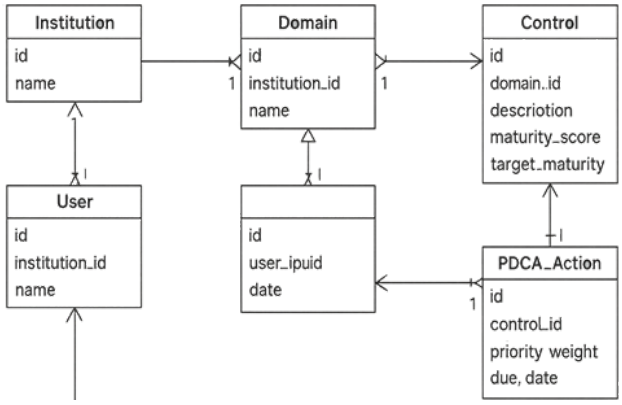

Figure 2. Simplified Entity-Relationship Diagram (ERD) for the CEM App

on control-level responses, prioritizes improvement actions using a weighted algorithm (priority_score = domain_weight * (target_maturity - current_maturity) * 10), and generates detailed assessments and planning reports.

The user interface, as shown in Figure 3, provides an intuitive dashboard that guides users through the complete PDCA workflow, from initial assessment and action planning to progress tracking and reassessment.

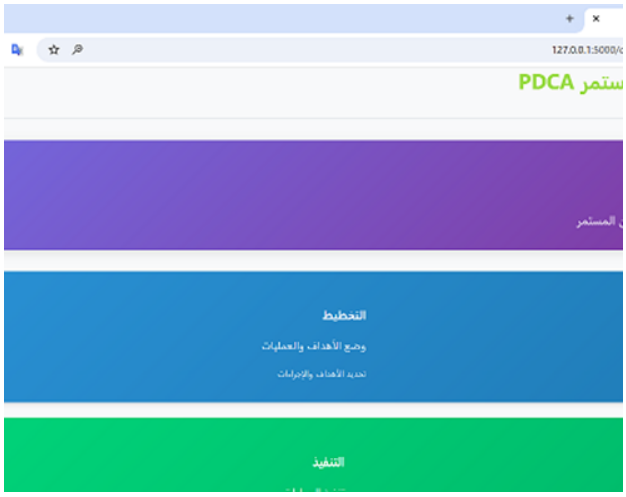

Figure 3. CEM Application Dashboard and PDCA Workflow Interface

8. DISCUSSION, IMPLICATIONS, AND FUTURE RESEARCH

8.1. Synthesis of Key Findings

This study empirically validates that cybersecurity in conflict-affected universities is a **predominantly socio-technical challenge**. The overwhelming correlation between *Awareness & Capacity Building* and readiness (r = .85) starkly contradicts a purely technical worldview and strongly supports the core STS tenet: human and organizational factors are the primary enablers (or blockers) of systemic change. The significant, moderate effect of holding a PhD (η^2 = 0.08) identifies this group as critical internal "change agents," whose expertise and credibility can be leveraged to champion the CEM's adoption, acting as a catalyst within often-hierarchical academic structures.

8.2. Theoretical and Practical Contributions

: This research contributes a **contextualized operationalization of STS Theory** for cybersecurity in resource-constrained environments. The CEM explicitly maps abstract STS principles (joint optimization, interdependence) onto concrete cybersecurity domains and processes, providing a template for similar adaptations in other sectors to follow.

Practically, it delivers a **prioritized, actionable roadmap**. The diagnostic data (e.g., low scores for business continuity) direct immediate action, whereas the CEM App reduces implementation complexity by automating assessment and planning. The findings offer clear guidance for leaders: investing in human capital and inclusive governance is foundational to technical success. The proposed model acknowledges constraints by advocating for phased, scalable interventions, starting with high-impact, low-cost measures in the Human-Centered Capacity Building and Inclusive Governance domains.

8.3. Limitations and Future Direction

This study has limitations that chart a course for future work. The cross-sectional design and focus on Sana'a limit causal inference and geographical generalizability of the findings. Future research should:

1. Employ **longitudinal designs** to track the impact of CEM implementation on actual security incidents and maturity over time.
2. Expand **geographical scope** within Yemen and conduct comparative studies with universities in similar conflict-affected states to refine the model's generalizability.
3. Adopt **mixed-methods approaches**, using qualitative interviews and focus groups to explore nuanced institutional barriers, leadership dynamics, and cultural factors that quantitative surveys cannot fully capture.
4. Conduct **technical validation studies** (e.g., controlled penetration tests, security audits) to triangulate and extend the self-reported data presented here, providing an objective measure of the model's impact on technical resilience.

9. CONCLUSION

In conclusion, this study moves beyond generic prescriptions to offer an empirically validated, context-sensitive framework for enhancing cybersecurity in one of the world's most challenging environments. By diagnosing critical gaps, revealing the paramount importance of human factors, and providing both a theoretical model (the CEM) and a practical tool (the CEM App), it bridges the critical gap between international cybersecurity standards and the realities of universities in conflict-affected regions. The path forward requires a fundamental shift in perspective: viewing cybersecurity not as an IT expense but as a socio-technical imperative integral to preserving institutional integrity, academic freedom, and mission continuity. The CEM provides a roadmap for this journey.

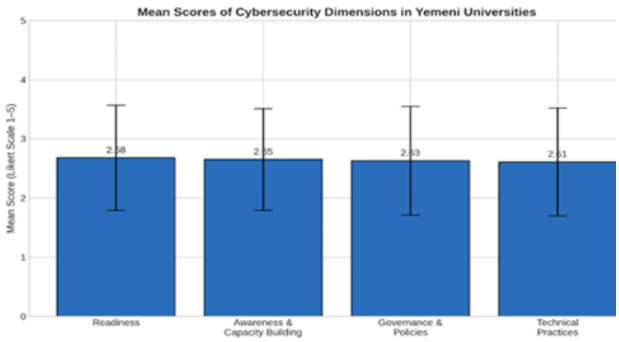

Figure 4. Is a vertical drawing (Bar Chart) showing the average scores of the four main dimensions (practices, governance, awareness, readiness).

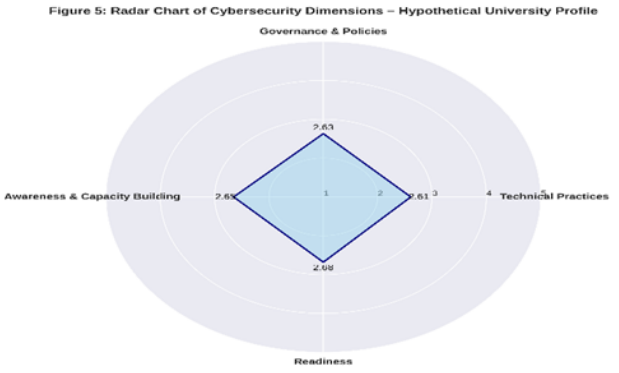

Figure 5. Radar Chart showing a hypothetical profile of a university based on the study results, which helps in comparative visualization.

REFERENCES

[1] N. Kshetri, "Cybersecurity in higher education: A global perspective," *J. Cybersecur.*, vol. 5, no. 1, tyz001, 2019.

[2] Educause, "Cybersecurity in higher education: Don't let the hackers win," *EDUCAUSE Rev.*, 2024.

[3] A. Al-Hadhrami, H. Al-Sharafi, and A. Al-Mashhadani, "Digital resilience in higher education in yemen," *Yemeni J. Comput. Sci. & Technol.*, 2021.

[4] F. E. Catota, M. G. Morgan, and D. C. Sicker, "Cybersecurity education in a developing nation: The ecuadorian environment," *J. Cybersecur.*, vol. 5, no. 1, tyz001, 2019.

[5] S. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. & Secur.*, vol. 38, pp. 97–102, 2013.

[6] ENISA, "Cybersecurity in the higher education sector: Good practices," European Union Agency for Cybersecurity, Tech. Rep., 2022.

[7] NIST, "Framework for improving critical infrastructure cybersecurity," National Institute of Standards and Technology, Tech. Rep. Version 1.1, 2018.

[8] ISO/IEC 27001, *Information security, cybersecurity and privacy protection — information security management systems — requirements*, International Organization for Standardization, 2022.

[9] M. Alshaikh, "Cybersecurity challenges and strategies in saudi arabian higher education institutions," *Int. J. Cyber Warf. Terror.*, vol. 10, no. 1, pp. 1–15, 2020.

[10] I. A. H. Humied, "Key determinants and strategies for cybersecurity education in yemen," *J. Digit. Educ. Train.*, vol. 7, no. 2, pp. 45–60, 2023.

[11] N. S. Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Comput. & Secur.*, vol. 56, pp. 70–82, 2016.

[12] E. C. K. Cheng and T. Wang, "Institutional strategies for cybersecurity in higher education institutions," *Information*, vol. 13, no. 4, p. 192, 2022.

[13] E. L. Trist and K. W. Bamforth, "Some social and psychological consequences of the longwall method of coal-getting," *Hum. Relations*, vol. 4, no. 1, pp. 3–38, 1951.

[14] M. Malatji, S. Von Solms, and A. Marnewick, "Socio-technical systems cybersecurity framework," *Inf. & Comput. Secur.*, vol. 27, no. 3, pp. 365–381, 2019.

[15] E. Zoto, M. Kianpour, and S. Kowalski, "A socio-technical systems approach to design and support systems thinking in cybersecurity and risk management education," *Complex Syst. Informatics Model. Q.*, vol. 18, pp. 1–15, 2019.

[16] C. W. Clegg, "Sociotechnical principles for system design," *Appl. Ergon.*, vol. 31, no. 5, pp. 463–477, 2000.

[17] D. Lakens, "Calculating and reporting effect sizes to facilitate cumulative science: A practical primer for t-tests and anovas," *Front. Psychol.*, vol. 4, p. 863, 2013.

[18] P. M. Podsakoff, S. B. MacKenzie, J. Y. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: A critical review of the literature and recommended remedies," *J. Appl. Psychol.*, vol. 88, no. 5, pp. 879–903, 2003.