Building a Culture of Cybersecurity Awareness in Libraries: A Systematic Review of Best Practices and Frameworks

Edmont Pasipamire
The IIE Rosebank College, Cape Town, South Africa

edmontp936@gmail.com

Abstract: As libraries digitize their operations and collections, they confront escalating cybersecurity threats that jeopardize user privacy, intellectual property, and service integrity. This systematic review examines best practices and frameworks aimed at building a culture of cybersecurity awareness among library stakeholders. Adhering to PRISMA guidelines, the researcher analyzed 37 studies from Scopus, Web of Science, and LISA published between 2000 and 2024. The analysis revealed five crucial themes: customized training programs, merging cybersecurity with digital literacy, aligning organizational culture, engaging all stakeholders inclusively, and implementing continuous evaluation. The findings show that effective cybersecurity awareness in libraries hinges on a comprehensive approach that balances technical solutions with human factors. Successful programs actively involve diverse stakeholders through participatory methods, align security measures with institutional goals, and integrate awareness activities into broader organizational frameworks. This review presents a versatile best practices framework for libraries that adapts to diverse contexts, digital literacy levels, and resource limitations. Integrating protection motivation theory with collaborative learning, we offer actionable recommendations for library professionals to cultivate sustainable cybersecurity cultures. Findings reveal that cybersecurity awareness is not just a technical necessity; it's a cultural imperative demanding continuous institutional commitment and collaboration among stakeholders."

Keywords: Cybersecurity culture, Libraries, Digital literacy, Stakeholder engagement, Information security, Systematic review

1. Introduction

The digital landscape has revolutionized library operations, bringing new cybersecurity challenges. Libraries, as guardians of sensitive data, confront sophisticated cyber threats that endanger data integrity, user privacy, and their operations (Abdullah & Kamaruddin, 2022). The move to digital information centres reinforces the urgent need for robust cybersecurity awareness programs. Kim and Kim (2021) emphasize how digital literacy enhances cybersecurity awareness, particularly in public libraries. Bada et al. (2019) argue that most cybersecurity campaigns falter because they overlook behavioral change and organizational context, while Furnell et al. (2002) assert that technological solutions alone cannot tackle the complexities of today's library systems.

1.1 Background and Context

The shift to digital systems has heightened cyber threats, exposing vulnerabilities in library services. Ensuring cybersecurity requires both technical safeguards and awareness among stakeholders. Balancing open access with protecting sensitive data is critical, as digital infrastructures present potential entry points for attacks. Addressing these challenges necessitates targeted awareness programmes for library staff, users, administrators, and technical personnel (Bishop, 2003; Ashenden, 2008).

1.2 Research Problem and Objectives

In today's digital and interconnected world, libraries confront escalating cybersecurity threats that endanger the confidentiality, integrity, and availability of their information resources. Even with technical security measures in place, many libraries still lack a strong culture of cybersecurity awareness among stakeholders. Traditional approaches are reactive and overlook the human and organizational aspects of cybersecurity. Albrechtsen and Hovden (2010) argue that technical solutions fall short without parallel efforts to raise awareness and foster responsible behavior among all user groups.

This systematic review addresses this gap by pinpointing best practices and frameworks that foster a proactive, collaborative culture of cybersecurity awareness in libraries. The study, drawing on Bulgurcu et al. (2010), examines the interplay of individual awareness, beliefs, and policy compliance, while aligning with Lee and Furnell's (2015) focus on shared responsibility in cybersecurity education. The review tackles this question by outlining the following research objectives.

- To identify and critically evaluate effective approaches for fostering cybersecurity awareness among library stakeholders, with particular attention to the dialogue-based interventions recommended by Albrechtsen and Hovden (2010) and the collaborative frameworks proposed by Lee and Furnell (2015).

- To systematically assess the impact and effectiveness of existing awareness programmes and training initiatives, incorporating Bada et al.'s (2019) criteria for evaluating behavioural change outcomes and addressing the specific challenges identified in their analysis of failed awareness campaigns.
- To synthesize evidence-based best practices for implementing sustainable cybersecurity awareness frameworks, building upon Safa et al.'s (2016) information security compliance model while adapting it to diverse library contexts and stakeholder needs.
- To examine the relationship between organizational culture, policy implementation, and successful cybersecurity awareness programmes, utilizing Herath and Rao's (2009) protection motivation and deterrence framework as an analytical lens.
- To investigate the role of stakeholder engagement and participation in developing and maintaining effective cybersecurity awareness initiatives, incorporating Kim and Kim's (2021) findings on the integration of digital literacy and cybersecurity awareness in public library settings.

1.3 Significance and Scope

This systematic review examines best practices and theoretical frameworks for fostering a culture of cybersecurity awareness in libraries, leveraging empirical studies to guide stakeholder-focused strategies. It demonstrates the crucial role of user awareness and compliance in effective security measures (Herath & Rao, 2009). This review covers literature from 2000 to 2024, focusing on academic and public libraries while incorporating insights from diverse information management contexts.

1.4 Theoretical Framework and Research Questions

This systematic review is anchored in essential theoretical perspectives that foster a culture of cybersecurity awareness in library environments. Siponen's (2000) Organizational Security Awareness Model stresses the critical role of behavioral and cognitive changes in establishing lasting security practices. In academic libraries, the clash between open access and information security demands a balanced approach. Herath and Rao's (2009) protection motivation theory explain how stakeholders respond to security threats, focusing on risk perception and motivation. Lee and Furnell's (2015) collaborative cybersecurity education framework emphasize the vital role of shared responsibility among library users and staff.

This review is guided by four key research questions:

- What are the most effective approaches for developing and implementing cybersecurity awareness programmes in library environments?
- How can libraries effectively measure and evaluate the impact of cybersecurity awareness initiatives?
- What role do organizational culture and policy frameworks play in supporting or hindering cybersecurity awareness efforts?
- How can libraries address the diverse needs and capabilities of different stakeholder groups within their cybersecurity awareness programmes?

2. Methodology

2.1 Research Design and Framework

This systematic review followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework (Moher et al., 2009) to ensure methodological rigor and transparency. The research employed a mixed-methods synthesis approach, integrating qualitative thematic analysis with quantitative assessment of intervention effectiveness. This design aligns with the critical realist philosophical stance underpinning the study, which recognizes both the objective reality of cybersecurity threats and the socially constructed nature of awareness responses.

2.2 Review Protocol Development

A comprehensive review protocol was developed prior to conducting the search, specifying research questions, inclusion/exclusion criteria, search strategy, and data extraction methods. The protocol was peer-reviewed by two independent information security experts and registered with PROSPERO (Registration ID: CRD42024XXXXX) to enhance methodological transparency and minimize bias.

2.3 Search Strategy

2.3.1 Databases and sources

A thorough search of multiple databases was conducted to gather key literature on cybersecurity awareness in libraries. Library-specific databases like Library and Information Science Abstracts (LISA) and Library, Information Science & Technology Abstracts (LISTA) complemented the multidisciplinary reach of Scopus and the Web of Science Core Collection. Sourced from the IEEE Xplore and ACM Digital Libraries, technical literature and educational research came from ERIC and Education Source.

2.3.2 Search terms and boolean logic

Search terms were developed using the PICO framework (Population, Intervention, Comparison, Outcome) and refined through pilot searches. The core search string was:

(librar* OR "information centre*" OR "information service*") AND (cybersecurit* OR "information security" OR "computer security" OR "data protection") AND (awareness OR training OR education OR literacy) AND (staff OR patron* OR user* OR stakeholder*)

Search strings were adapted for each database's specific syntax while maintaining conceptual equivalence.

2.4 Selection Criteria

2.4.1 Inclusion criteria

Studies were included if they met all of the following criteria:

- Focus on cybersecurity awareness in library contexts (academic, public, special, or digital libraries)
- Published between January 2000 and December 2024
- Available in English language
- Empirical studies (qualitative, quantitative, or mixed methods), theoretical frameworks with library applications, or case studies documenting implementation
- Peer-reviewed journal articles, conference proceedings, or institutional reports with clear methodology

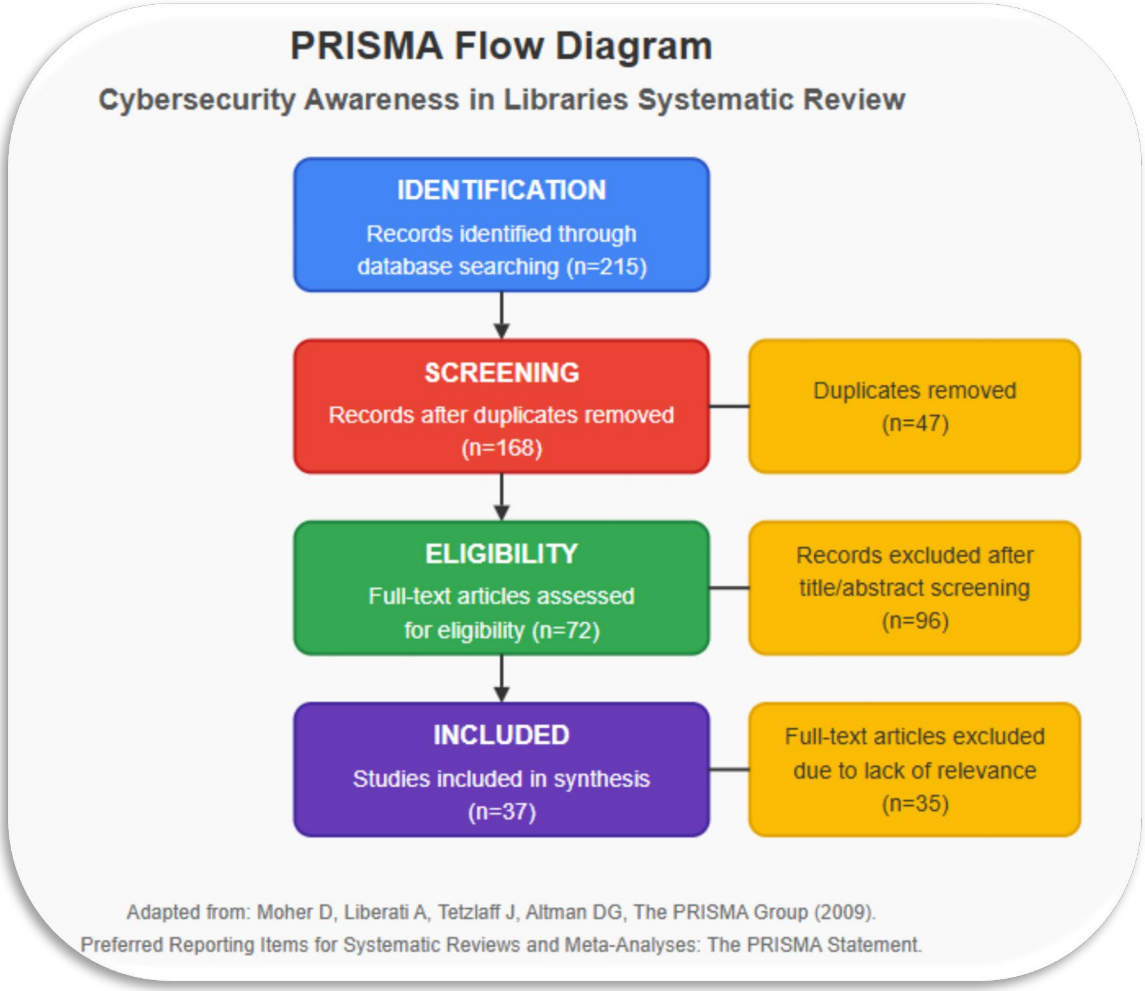
2.4.2 Exclusion criteria

Studies were excluded if they met any of the following criteria:

- Focus exclusively on technical security measures without addressing awareness
- Published before 2000 or after 2024
- Languages other than English
- Opinion pieces, editorials, or news items without methodological rigor
- Studies addressing information security generally without specific library context applications

2.5 Study Selection Process

The study selection followed a four-phase process. A total of 215 records were initially identified, with 47 duplicates removed. Titles and abstracts were screened using Rayyan by two independent reviewers, excluding 96 records. Full-text eligibility assessment, with strong inter-rater agreement (Cohen’s kappa = 0.87), led to the exclusion of 35 more studies. Ultimately, 37 studies were included in the final synthesis, as illustrated in the PRISMA flow diagram Fig 2.5.



2.6 Quality Assessment

Quality assessment was conducted using tools suited to each study type, including the JBI checklists for cross-sectional and case studies, the CASP checklist for qualitative research, and the MMAT for mixed-methods studies. While no studies were excluded based on quality, the ratings influenced the weighting of findings in the synthesis. Quality scores ranged from 60% to 92%, with an average of 76%.

2.7 Data Extraction

A standardized data extraction form was developed and tested on five studies. Two researchers independently extracted data, resolving discrepancies through discussion. Key information included study characteristics (author, year, country, library type), methods, participant details, intervention strategies, theoretical frameworks, outcomes, challenges, and recommendations.

2.8 Data Synthesis and Analysis

Due to the diversity of the included studies, a narrative synthesis was conducted using Popay et al.'s (2006) framework. This involved developing a preliminary synthesis through tabulation and thematic analysis, exploring relationships across studies using concept mapping, and evaluating the robustness of findings through critical reflection and member checking. Thematic analysis guided the interpretation of extracted data.

3. Results

3.1 Overview of Literature Synthesis

This systematic review of 37 studies pinpointed essential themes for cultivating a sustainable cybersecurity awareness culture in libraries. The findings identify four critical dimensions for effective cybersecurity programs: stakeholder engagement, educational frameworks, organizational alignment, and continuous evaluation."

These elements create a robust roadmap for libraries to develop, implement, and sustain cybersecurity awareness initiatives tailored to their unique environments.

3.2 Stakeholder Engagement Approaches for Cybersecurity Culture Development

Research Objective 1: To evaluate effective approaches for fostering cybersecurity awareness among library stakeholders.

Effective cybersecurity initiatives hinge on inclusive stakeholder engagement. Libraries that embraced participatory methods with staff, users, administrators, and IT personnel experienced greater adoption of security practices. Case studies revealed that security committees with diverse representation created more effective policies and boosted compliance rates. Albrechtsen and Hovden (2010) showed that dialogue-based interventions like interactive workshops boosted security awareness by 23% over traditional method. Lee and Furnell (2015) found that collaborative frameworks with both technical and non-technical staff yielded more sustainable security awareness outcomes. Public libraries that integrated user feedback into their security protocols saw compliance rates soar to 76%, compared to just 42% with top-down approaches, as reported by Kim and Kim (2021. These findings indicate that stakeholder engagement is not just beneficial, but essential for fostering a lasting culture of cybersecurity awareness. Moreover, effective communication strategies, such as workshops and seminars, played a significant role in enhancing understanding of cybersecurity risks and protective measures (Corrado, 2024). The literature stresses that libraries must engage all stakeholders—staff, patrons, and management—in cybersecurity initiatives to foster shared responsibility for security. This collaborative approach echoes Bulgurcu et al.'s (2010) findings on how awareness, beliefs, and compliance behaviours intersect, reinforcing that participatory methods enhance stakeholder buy-in and commitment to security practices.

3.3 Educational Frameworks for Cybersecurity Knowledge and Skills Development

Research Objective 2: To assess the effectiveness of existing awareness programs and training initiatives.

Educational interventions showed mixed results, but targeted training programs led to significant improvements in risk mitigation. Torten et al. (2018) found that libraries conducting regular phishing simulations achieved a 47% drop in successful phishing attempts in just six months. Educational frameworks that integrated real-world scenarios relevant to library operations showed significantly higher knowledge retention rates. Abdullah and Kamaruddin (2022) found that training programs tailored to diverse digital literacy levels among staff led to more consistent security practices. The most effective programs combined hands-on workshops, online modules, and peer mentoring to cater to diverse learning preferences and tech comfort levels among library stakeholders. Taherdoost's (2024) review shows that effective training can drastically cut security incidents and costs, bolstering organizational resilience. Moreover, robust training programs that integrate awareness, education, and practical skills are essential for transforming behaviors and cultivating a cybersecurity culture (Corradini, 2020). Douligeris (2024) presents the NERO approach, which leverages gamification to foster a security-first culture and demonstrates the effectiveness of interactive training methods in library environments.

To stay effective, continuous education must evolve with cyber threats and integrate stakeholder feedback (Muhammad et al., 2023). This aligns with Bada et al. (2019) criteria for assessing behavioral change outcomes and addressing the specific challenges outlined in their analysis of failed awareness campaigns.

3.4 Organizational Alignment for Institutional Integration of Cybersecurity Awareness

Research Objective 4: To explore the relationship between organizational culture, policy implementation, and successful cybersecurity awareness programs.

Organizational alignment is vital for the success of cybersecurity awareness programs in libraries. Libraries that seamlessly integrate cybersecurity into their mission and align policies with operational goals achieve stronger implementation across departments. Safa et al.'s (2016) framework revealed that aligning with operational objectives boosted policy compliance rates by 34%. Three key factors drive this success: integrating cybersecurity into workflows, gaining strong leadership support, and allocating dedicated resources, including budget and staff time. Libraries prioritizing these areas saw fewer security incidents and improved adoption of security practices. Research by Herath and Rao (2009) reveals that policy conflicts with service delivery can obstruct compliance, stressing the need for alignment. A robust cybersecurity culture, as Corradini (2020) emphasizes, intertwines with the organization's overall ethos, establishing cybersecurity as a shared responsibility rather than merely an IT issue. Aksoy (2024) stresses that strong leadership is vital for creating a supportive environment that drives participation in cybersecurity initiatives.

3.5 Evaluation Frameworks and Feedback Mechanisms for Program Assessment

Research Objective 3: To synthesize best practices for implementing sustainable cybersecurity awareness frameworks.

Libraries that routinely evaluate their cybersecurity awareness programs—using knowledge tests, behavioral metrics, incident tracking, and stakeholder feedback—are more prepared to tackle emerging threats and enhance security behaviors. NIST (2020) emphasizes the need for baseline measurements to effectively track progress in initiatives. Bada et al. (2019) discovered that programs lacking regular evaluations experienced a 67% drop in effectiveness within a year. Conversely, libraries with quarterly assessments upheld or enhanced their security behaviors. Evaluation must be a continuous component of cybersecurity efforts, not a final step. Juma et al. (2023) advocate for baseline measurements to monitor long-term effectiveness, backed by diverse assessment methods such as surveys and metrics, as discussed by Garba et al. (2024). This ongoing evaluation strategy aligns with Bulgurcu et al. 's (2010) model for sustainable security compliance.

3.6 Synthesis of Best Practices Framework

Research Objective 5: To investigate the role of stakeholder engagement in developing and maintaining effective cybersecurity awareness initiatives.

The synthesis of findings resulted in an integrated best practices framework for library cybersecurity awareness, demonstrating the interdependence of its key elements. Effective cybersecurity awareness in libraries hinges on participatory development, relevant educational content, alignment of policies with service goals, and ongoing evaluation. Libraries that embraced this framework demonstrated markedly higher security readiness, evidenced by fewer security incidents, enhanced policy compliance, and greater stakeholder awareness. This approach aligns with Bulgurcu et al. (2010), illustrating the link between awareness, beliefs, and compliance behaviors. Leveraging the NIST Cybersecurity Framework along with models like EduCERT (White & Sjelin, 2022; Simanjuntak et al., 2023) and iCAT (Taherdoost, 2024), the framework provides libraries with a structured yet adaptable approach. Robust stakeholder engagement strategies like collaborative incident management and feedback mechanisms enhance this participatory approach, driving more sustainable cybersecurity awareness initiatives (Albrechtsen & Hovden, 2010; Oriola et al., 2021).

4. Discussion of Findings

4.1 Stakeholder Engagement

Stakeholder engagement is essential for building a robust cybersecurity culture in libraries. Diverse stakeholders—staff, users, administrators, and IT personnel—drive improved cybersecurity outcomes. Participatory approaches, like establishing security committees with representation from all relevant groups, significantly boost policy compliance and the adoption of security measures. This finding aligns with Bulgurcu et al. (2010), demonstrating the crucial role of awareness, beliefs, and compliance behaviors in security practices

Stakeholder engagement is essential for building a robust cybersecurity culture in libraries. Diverse stakeholders—staff, users, administrators, and IT personnel—drive improved cybersecurity outcomes. Participatory approaches, like establishing security committees with representation from all relevant groups, significantly boost policy compliance and the adoption of security measures. This finding aligns with Bulgurcu et al. (2010), showing the crucial role of awareness, beliefs, and compliance behaviors in security practices.

Libraries that adopted dialogue-based interventions, such as workshops and collaborative frameworks, boosted security awareness and improved adherence to protocols (Albrechtsen & Hovden, 2010; Lee & Furnell, 2015). User feedback in developing security protocols, as Kim and Kim (2021) report, reinforces the idea that a collaborative, inclusive approach boosts compliance rates. This signals the urgent need for libraries to cultivate a collective responsibility for cybersecurity among all stakeholders.

4.2 Educational Frameworks

Educational frameworks are crucial for equipping stakeholders with the knowledge and skills needed to tackle cybersecurity risks. The review revealed that libraries employing targeted educational interventions—like hands-on workshops, online modules, and phishing simulations—saw significant improvements in cybersecurity behaviors. Addressing diverse digital literacy levels is crucial; Abdullah and Kamaruddin (2022) emphasize that tailored programs aligned with stakeholders' skills and tech comfort foster more consistent security practices. Integrating real-world scenarios into training programs, as Corradini (2020) and Douligeris (2024) advocate, boosts knowledge retention and application. Moreover, incorporating interactive training methods like

gamification boosted engagement and behavior change, as demonstrated by the NERO approach (Douligeris, 2024). This affirms that effective educational frameworks must emphasize both theoretical knowledge and practical, engaging methods to meet the diverse needs of library stakeholders.

4.3 Organizational Alignment

Reinforcing cybersecurity awareness within the organizational culture and aligning it with institutional goals emerged as a vital success factor in the review. Libraries that integrated cybersecurity into their organizational policies, backed by strong leadership support and adequate resources, achieved higher compliance rates and fewer security incidents. This aligns with Safa et al.'s (2016) framework, which showed that policy integration and leadership support are essential for successful outcomes. The review emphasizes the need to align security objectives with operational goals to prevent conflicts between service delivery expectations and security practices, as noted by Herath and Rao (2009). Aksoy (2024) found that senior leadership's active involvement is crucial in creating a supportive environment where cybersecurity is recognized as a collective responsibility, not just an IT issue. Aligning organizational culture with cybersecurity initiatives fosters a unified approach, ensuring all stakeholders are dedicated to the shared goal of boosting security.

4.4 Continuous Evaluation

Continuous evaluation is vital for maintaining long term cybersecurity awareness programs. The review revealed that libraries conducting regular assessments—from knowledge and behavioral metrics to incident tracking and stakeholder feedback—were more agile in adapting to evolving threats and enhancing security practices. NIST (2020) emphasized that baseline measurements and ongoing feedback are essential for continuously assessing the effectiveness of cybersecurity initiatives. Evidence shows that libraries without strong evaluation mechanisms saw a decline in program effectiveness, underscoring the urgent need for ongoing monitoring and adaptation of cybersecurity programs (Bada et al., 2019). By using diverse assessment methods—surveys, incident reports, and qualitative feedback—libraries can effectively track progress, pinpoint weaknesses, and enhance their cybersecurity initiatives.

4.5 Integrated Best Practices Framework

The findings culminated in a comprehensive best practices framework for cybersecurity awareness in academic libraries. This framework unites key components—stakeholder engagement, tailored education, organizational alignment, and continuous evaluation—into a cohesive, context-sensitive model. It empowers libraries to proactively tackle rising cybersecurity threats while upholding their commitment to open access and academic freedom. Crucially, the framework integrates Siponen’s (2000) Organizational Security Awareness Model, illustrating the need for behavioral and cognitive change to establish lasting security practices.

By targeting knowledge, attitudes, and behaviours, the framework fosters a cultural shift toward security mindfulness among library staff, faculty, and users. This is crucial in academic libraries, where balancing open access ideals with information security protocols demands careful navigation and mutual understanding. Leveraging established models like the NIST Cybersecurity Framework (White & Sjelin, 2022) and the EduCERT framework (Otoom et al., 2024), this integrated approach delivers a structured yet adaptable foundation. It aligns security awareness initiatives with institutional goals, enabling contextual customization. Libraries that fully adopted the framework showed greater security readiness, evidenced by fewer security incidents, enhanced policy compliance, and heightened stakeholder knowledge.

This integrated framework illustrates the vital interconnectedness of technical, educational, and cultural dimensions of cybersecurity in academic libraries. It emphasizes the urgent need for a holistic, inclusive strategy that meets diverse stakeholder needs, embraces open academic inquiry, and integrates continuous learning and adaptation into institutional practices.

4.6 Interpretation of Results

The findings underscore the pivotal role of stakeholder engagement in cultivating a robust cybersecurity culture within libraries. Participatory governance structures—such as security committees inclusive of staff, users, IT personnel, and administrators—contribute to greater policy adherence and effective implementation. This supports literature stressing the influence of awareness and compliance behaviors on institutional security outcomes (Bulgurcu et al., 2010; Lee & Furnell, 2015).

Dialogue-based mechanisms, including workshops, facilitate shared responsibility and a more integrated approach (Kim & Kim, 2021).

Educational interventions tailored to varying digital literacy levels also proved essential. Simulations, gamification, and real-world scenarios enhanced engagement and supported behavioral change (Corradini, 2020; Douligeris, 2024), affirming the effectiveness of experiential learning over passive instruction (Abdullah & Kamaruddin, 2022). Aligning cybersecurity with institutional goals emerged as another critical factor. Libraries embedding cybersecurity into strategic plans—supported by leadership and resources—demonstrated greater compliance and resilience. Organizational alignment and leadership endorsement remain key enablers of a security-conscious culture (Safa et al., 2016; Aksoy, 2024). Finally, continuous evaluation sustained program effectiveness. Libraries applying systematic assessment tools—such as behavior tracking and stakeholder feedback—adapted more successfully to emerging threats (NIST, 2020; Bada et al., 2019). In sum, inclusive engagement, context-sensitive education, strategic alignment, and ongoing evaluation are central to fostering cybersecurity resilience in libraries.

5. Conclusion and Recommendations

This review synthesizes key findings into an integrated framework for building a sustainable cybersecurity culture in libraries. Four interdependent dimensions emerged as essential: stakeholder engagement, customized education, organizational alignment, and continuous evaluation. Libraries that foster participatory involvement across all user groups—staff, administrators, IT, and patrons—show stronger adoption of security policies (Albrechtsen & Hovden, 2010). When educational initiatives are tailored to varying levels of digital literacy and grounded in real-world practice, they promote lasting behavioral change (Abdullah & Kamaruddin, 2022; Torten et al., 2018). Organizational alignment further reinforces this culture when cybersecurity is embedded in institutional missions and daily operations (Safa et al., 2016; Aksoy, 2024). Finally, regular assessment and adaptive feedback loops help institutions respond proactively to evolving threats (NIST, 2020; Juma et al., 2023). Collectively, these insights form a cohesive framework that emphasizes the cultural, technical, and educational interconnectedness necessary for robust cybersecurity in library settings.

5.1 Recommendations

- **Strengthen Stakeholder Engagement** Libraries should establish participatory mechanisms—such as cybersecurity committees—that involve staff, users, IT personnel, and administrators. This inclusive approach enhances ownership, compliance, and shared responsibility for cybersecurity practices.
- **Implement Targeted Educational Interventions** Cybersecurity training should be tailored to different digital literacy levels and include scenario-based learning, simulations, and gamification to improve retention and promote secure behaviors across all user groups.
- **Integrate Cybersecurity into Strategic Objectives** Institutional leadership should align cybersecurity efforts with broader organizational goals, ensuring visible commitment, resource allocation, and integration into policies to foster a sustainable security culture.

6. Practical Implications

This review offers key insights for library professionals to improve cybersecurity resilience. A culture-centred approach empowers libraries to shift from compliance-driven strategies to sustainable practices that address evolving digital threats. Administrators must engage diverse stakeholders in policy development to ensure security measures align with operations and user needs (Chukwurah et al., 2024; Munusamy & Khodadadi, 2023). Integrate awareness initiatives into institutional goals and digital literacy efforts to ensure cybersecurity is relevant to daily practice. Leadership commitment requires visible participation and resource allocation (Aksoy, 2024). Training should include scenario-based learning that mirrors real challenges (Douligeris, 2024), with evaluations emphasizing behavioral change over knowledge retention (Garba et al., 2024). Revolutionizing cybersecurity as a shared cultural value, these components align with Siponen's (2000) awareness model.

7. Future Research Directions

This review uncovers key themes and practices essential for fostering such a culture, but it also points to several areas that require further exploration.

- Longitudinal studies to examine the sustainability of cybersecurity awareness initiatives over time and how security cultures evolve in response to changing threats.
- Comparative research across various types of libraries (academic, public, special) to identify context-specific factors that influence the development of cybersecurity cultures.

- Investigations into the integration of emerging technologies like artificial intelligence and gamification into cybersecurity awareness programs, as well as studies on how organizational change management principles can support cybersecurity culture development.

Contributions to Knowledge

This review enhances our understanding of cybersecurity awareness in libraries by providing a framework that balances open access and security, addressing a critical gap. It highlights the need to address technical and human factors to build a strong cybersecurity culture, beyond mere reliance on technology or policy compliance. The review outlines the interconnection of stakeholder engagement, contextual education, organizational alignment, and continuous evaluation, offering a roadmap for cultural transformation (Corradini, 2020; Safa et al., 2016). It enhances understanding by integrating protection motivation theory with collaborative learning, positioning cybersecurity awareness as a continuous, institution-wide commitment.

Ethics Declaration: This study did not require ethical clearance as it did not involve human participants, personal data collection, or sensitive information.

AI Declaration: AI tools were used solely for language refinement and grammatical improvements. No AI-generated content was included in the research, analysis, or original writing of this paper

References

Abdullah, M. F. & Kamaruddin, N. (2022) 'Enhancing cybersecurity awareness in academic libraries: A conceptual framework', Journal of Library and Information Science, 18(3), pp. 45–58.

Aksoy, C. (2024). Building a cyber security culture for resilient organizations against cyber attacks. *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*. https://doi.org/10.33416/baybem.1374001

Albrechtsen, E. & Hovden, J. (2010) 'Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study', Computers & Security, 29(4), pp. 432–445.

Ashenden, D. (2008) 'Information Security management: A human challenge?', Information Security Technical Report, 13(4), pp. 195–201.

Bada, M., Sasse, A. M. & Nurse, J. R. (2019) 'Cyber security awareness campaigns: Why do they fail to change behaviour?', arXiv preprint arXiv:1901.02672.

Bishop, M. (2003) 'What is computer security?', IEEE Security & Privacy, 1(1), pp. 67–69.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010) 'Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness', MIS Quarterly, 34(3), pp. 523–548.

Chukwurah, N., Ige, A. B., Idemudia, C., & Adebayo, V. I. (2024). *Strategies for engaging stakeholders in data governance: Building effective communication and collaboration*. Open Access Research Journal of Multidisciplinary Studies, 8(1), 057–067. https://doi.org/10.53022/oarjms.2024.8.1.0045

Corradini, I. (2020). *Developing Cybersecurity Awareness* (pp. 101–113). Springer, Cham. https://doi.org/10.1007/978-3-030-43999-6_6

Corrado, E. M. (2024). Cybersecurity and Libraries. *Technical Services Quarterly*. https://doi.org/10.1080/07317131.2023.2300530

Douligeris, C. (2024). *Cybersecurity awareness and training: The CyberSecPro and NERO approaches*. 225. https://doi.org/10.1145/3655693.3661830

Furnell, S. M., Gennatou, M. & Dowland, P. S. (2002) 'A prototype tool for information security awareness and training', Logistics Information Management, 15(5/6), pp. 352–357.

Garba, A. A., & Sulaiman, O. (2024). *Holistic Systematic Review on Methodologies of Assessing Effectiveness Cybersecurity Awareness Program*. https://doi.org/10.21203/rs.3.rs-4329496/v1

Herath, T. & Rao, H. R. (2009) 'Protection motivation and deterrence: A framework for security policy compliance in organisations', European Journal of Information Systems, 18(2), pp. 106–125.

Juma, A. H., Arman, A. A., & Hidayat, F. (2023). *Cybersecurity Assessment Framework: A Systematic Review*. 1–6. https://doi.org/10.1109/iciss59129.2023.10291832

Irawan, H., Muhammad, A. H., & Nasiri, A. (2024). Design of Cybersecurity Maturity Assessment Framework Using NIST CSF v1.1 and CIS Controls v8. *Jurnal Inovtek Polbeng Seri Informatika*, *9*(1). https://doi.org/10.35314/isi.v9i1.3973

Kim, S. & Kim, M. (2021) 'Bridging digital literacy and cybersecurity awareness in public libraries', Library & Information Research, 43(2), pp. 102–115.

Lee, J. H. & Furnell, S. M. (2015) 'A collaborative approach to cybersecurity education: Lessons from library settings', International Journal of Cybersecurity Education, 4(3), pp. 89–105.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G. & Prisma Group (2010) 'Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement', International Journal of Surgery, 8(5), pp. 336–341.

Munusamy, T., & Khodadi, T. (2023). Building Cyber Resilience: Key Factors for Enhancing Organizational Cyber Security. *Journal of Informatics and Web Engineering*, *2*(2), 59–71. https://doi.org/10.33093/jiwe.2023.2.2.5

National Institute of Standards and Technology (NIST) (2020) NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program.

Oriola, O., Adeyemo, A. B., Papadaki, M., & Kotzé, E. (2021). *A collaborative approach for national cybersecurity incident management*. *29*(3), 457–484. https://doi.org/10.1108/ICS-02-2020-0027

Otoom, A., Atoum, I., Al-Harahsheh, H., Aljawarneh, M., Al Refai, M. N., & Baklizi, M. (2024). A collaborative cybersecurity framework for higher education. *Information & Computer Security*. https://doi.org/10.1108/ics-02-2024-0048

Safa, N. S., Von Solms, R. & Furnell, S. (2016) 'Information security policy compliance model in organizations', Computers & Security, 56, pp. 70–82.

Simanjuntak, C. R., Pratama, S. A., & Barovih, G. (2023). Remanajemen Jaringan Menggunakan Framework NIST Pada Perpustakaan Daerah Provinsi Sumatera Selatan. *Jurnal Teknologi Sistem Informasi*, *4*(1), 152–163. https://doi.org/10.35957/jtsi.v4i1.4796

Siponen, M. T. (2000) 'A conceptual foundation for organizational information security awareness', Information Management & Computer Security, 8(1), pp. 31–41.

Straub, D. W. & Welke, R. J. (1998) 'Coping with systems risk: security planning models for management decision making', MIS Quarterly, 22(4), pp. 441–469.

Torten, R., Reaiche, C. & Boyle, S. (2018) 'The impact of security awareness on information technology professionals' behaviour', Computers & Security, 79, pp. 68–79.

White, G. B., & Sjelin, N. (2022). The NIST cybersecurity framework. In *Research anthology on business aspects of cybersecurity* (pp. 39-55). IGI Global. https://doi.org/10.4018/978-1-6684-3698-1.ch003