International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Literature Review - A Study on Impact of Cyber Security on Organisation Culture and Structure with Reference to Public Sector Bank

Anuja A. Patil[1], Dr. Mohasin A. Tamboli[2]

[1]Research Scholar, PIRENS Institute of Business Management and Administration, Loni, A. Nagar, Savitribai Phule university, Pune.
Email: *anujapatil2107[at]gmail.com*

[2]Associate Professor, PIRENS Institute of Business Management and Administration, Loni, A. Nagar, Savitribai Phule university, Pune.
Email: *mohasinat[at]gmail.com*

Abstract: ***The rapid advancement of digital technologies has significantly increased cyber-security risks across all sectors, compelling organisations to strengthen their security frameworks. In public sector banks, where large volumes of sensitive financial data are managed, cyber-security has become a critical determinant shaping organisational culture and structure. This literature review examines existing research on the impact of cyber-security practices on organisational culture and structure, with specific reference to public sector banks. Findings from prior studies indicate that cyber-security initiatives influence employee behaviour, awareness levels, communication patterns, and the overall risk culture within organisations. Strengthened security protocols often lead to more formal, compliance-driven cultures, as well as structural adjustments such as specialised cyber-security units, hierarchical decision-making processes, and redesigned reporting mechanisms. The review also highlights that while robust cyber-security enhances trust, accountability, and operational resilience, it can also introduce challenges such as employee resistance, increased workload, and the need for continuous training. By synthesising key themes from the literature, this review underscores the evolving relationship between cyber-security, organisational culture, and structure in public sector banks, offering insights relevant for enhancing organisational effectiveness and security readiness.***

Keywords: Cyber security, Organization Culture, Organization structure, public sector bank

1. Introduction

In the digital era, cyber security has emerged as a critical concern for organisations across all industries. Public sector banks, in particular, manage highly confidential financial information and serve millions of customers, making them prime targets for cyber threats. The increasing frequency and sophistication of cyber-attacks have compelled these institutions to invest heavily in security technologies, policies, and practices. As a result, cyber security is no longer viewed solely as a technical function; it has become an essential organisational priority that influences strategic planning, daily operations, and employee behaviour.

The evolving risk landscape has led public sector banks to re-examine their organisational culture and structure. Cyber security frameworks require strict compliance, vigilance, continuous monitoring, and strong risk awareness among employees. This shift often results in more formalised and rule-based cultures, greater accountability, and enhanced internal controls. At the structural level, banks are increasingly establishing dedicated cyber security departments, revising reporting hierarchies, and adopting hybrid or centralised structures to improve security oversight and response mechanisms.

This literature review explores how cyber security practices shape the cultural and structural dimensions of public sector banks. It draws on existing research to identify key themes such as risk awareness, employee attitudes, training and capacity building, organisational change, and structural adaptation. The review also highlights gaps in current studies, particularly in understanding the behavioural and cultural implications of cyber security measures in public financial institutions.

By examining the interplay between cyber security, organisational culture, and structure, this review offers insights into how public sector banks can strengthen resilience, enhance employee engagement, and build a secure, adaptive organisational environment. The introduction sets the foundation for analysing the broader academic discourse on the subject and contributes to the growing body of knowledge in organisational and security studies.

2. Objectives of study

1) To study the concept of cyber security, Organizational Culture, organisation structure.
2) To study the impact Impact of cyber security on organisation culture and structure with reference to public sector bank

3. Research Methodology

The research methodology for this literature review is based entirely on a qualitative and descriptive approach, relying on secondary data to explore the impact of cyber security on organisational culture and structure in public sector banks. The study systematically collects and analyses previously published academic work, drawing information from peer-reviewed journals, books, government reports, RBI guidelines, CERT-In publications, and credible online databases such as Google Scholar, JSTOR, ResearchGate, and Elsevier. A structured keyword search was carried out using terms such as “cyber security in banks,” “organisational

culture," "organisational structure," "public sector banks," "cyber risk management," and "security compliance," combined through Boolean operators to refine relevant results. The inclusion criteria focused on literature published between 2010 and 2024, studies related to cyber security practices and organisational behaviour, and research specifically linked to the banking sector, while sources lacking academic credibility, non-English publications, and purely technical cyber security papers were excluded. The collected literature was reviewed through a thematic analysis method that identified major patterns, recurring concepts, and emerging themes such as risk awareness, compliance culture, organisational restructuring, training needs, and governance improvements. This methodology ensures a comprehensive synthesis of existing knowledge while highlighting gaps and variations across studies. However, the review is limited by its dependence on secondary data, restricted access to some paid journals, and the limited availability of India-specific research on public sector banks. All sources were used ethically, with respect for academic integrity and proper citation practices.

4. Literature Review

According to Dhillon, G. (2015) that work highlights the significance of organisational behaviour and culture in shaping cyber security practices. He argues that security is not just a technical issue but a behavioural one influenced by employee attitudes, trust levels, and leadership commitment.

A Study by Parsons, K. et al. (2017) Stated that Parsons and colleagues emphasise the role of security awareness among employees. Their research shows that organisational culture directly affects employee compliance with cyber security policies, making training and awareness crucial.

A Study by Von Solms, R. & Van Niekerk, J. (2013) stated that Their study presents a holistic, human-centered view of cyber security, showing how organisational culture determines the success of security frameworks. They identify the need for cultural adaptation to support evolving security demands.

According to Schein, E. H. (2010) that Schein's foundational research on organisational culture provides a theoretical base for understanding how cyber security policies shape norms, values, and behaviour within institutions such as banks.

According to Alshaikh, M. (2020) that Alshaikh focuses on the development of a cyber security culture model, arguing that organisations require structured cultural frameworks to effectively manage security risks. His model is widely used in banking research.

A study by Ifinedo, P. (2014) stated that Ifinedo examines the behavioural aspects of cyber security policy compliance in organisations. He finds that organisational support, management involvement, and security climate significantly affect compliance behaviour.

A study by Ponemon Institute (2018) stated that Industry-based empirical studies by the Ponemon Institute reveal how cyberattacks influence organisational structure and governance. Their findings show that banks respond to cyber threats by establishing specialised cyber security units and new reporting mechanisms.

According to National Institute of Standards and Technology (NIST) 's Authors: Ross, McEvilley & Oren (2016) stated that The NIST Cyber Security Framework demonstrates how organisations redesign structures and processes to align with risk-based decision-making. Banks globally follow this model to improve security governance.

A study by Rao, S. & Sahu, G. (2013) suggested that the IT security practices in Indian banks, showing that public sector banks face unique cultural barriers such as resistance to change, lack of awareness, and bureaucratic structures that slow implementation.

According to Reserve Bank of India- RBI Working Papers (Various Authors, 2017–2022) RBI's research and guidelines highlight how cyber security requirements reshape bank structures, mandate cyber security committees, and promote cultural shifts toward compliance, risk awareness, and accountability.

5. Theoretical framework

The theoretical framework for this literature review is grounded in organisational theory, behavioural theory, and cyber security culture models that explain how security practices influence the culture and structure of public sector banks. The foundation of the framework draws on Schein's Theory of Organisational Culture, which states that shared values, beliefs, and behavioural norms shape how employees respond to organisational priorities such as cyber security. According to this theory, the introduction of stricter security policies, awareness programs, and compliance mechanisms transforms underlying cultural assumptions and encourages a more risk-aware environment. Additionally, the review uses Contingency Theory to explain how organisations modify their structures in response to external threats and technological changes; cyber-attacks and regulatory requirements act as contingencies that push banks toward more formalised, centralised, and technology-driven structures. Socio-Technical Systems Theory further supports the idea that technological advancements like cyber security tools must align with human and social components to be effective. This theory helps explain why employee behaviour, attitudes, and training influence the success of cyber security initiatives. The framework is also supported by the Cyber Security Culture Model (Alshaikh, 2020), which highlights how leadership, communication, and policy enforcement contribute to developing a strong security culture. Together, these theories establish that cyber security is not merely a technical function but a strategic organisational element that reshapes both cultural dynamics and structural arrangements within public sector banks. This integrated framework guides the analysis of how cyber security measures influence organisational behaviour, decision-making processes, communication patterns, hierarchy, and overall governance in the banking context.

6. Findings and Discussion

The findings of the literature review reveal that cyber security has become a central factor influencing both organisational culture and organisational structure in public sector banks. Across the literature, a consistent theme emerges: the growing sophistication of cyber threats has compelled banks to strengthen their internal security frameworks, resulting in a more compliance-oriented and risk-aware culture. Studies indicate that cyber security initiatives—such as mandatory training, policy enforcement, and continuous monitoring—have reshaped employee attitudes, promoting vigilance, accountability, and adherence to standard procedures. However, the literature also highlights challenges such as employee resistance, limited awareness, and a traditional bureaucratic mindset that often slows the adoption of security-driven cultural changes in public sector banks. Structurally, the review finds that banks have increasingly created specialised cyber security departments, revised reporting hierarchies, and adopted centralised decision-making models to improve incident response and regulatory compliance. Research further suggests that organisational structures have shifted toward integrating technology, governance, and risk management functions more closely, reflecting a move from traditional functional structures to hybrid or security-integrated frameworks. Many researchers agree that effective cyber security requires aligning structural changes with cultural transformation; technology alone cannot ensure security unless employees internalise security values and management actively supports a security-oriented climate. The literature also discusses the influence of external factors such as RBI guidelines, legal mandates, and global security standards, which push public sector banks to adopt more formal, structured, and technology-driven operational models. Overall, the findings suggest a strong interdependence between cyber security practices, organisational culture, and organisational structure, with both cultural and structural dimensions evolving in response to rising cyber risks and regulatory pressures. The discussion highlights that while progress has been made, public sector banks still need to strengthen employee engagement, enhance security awareness, and streamline structures to achieve a mature cyber security culture capable of supporting long-term resilience and organisational effectiveness.

7. Recommendations

Based on the literature reviewed, it is recommended that public sector banks strengthen their cyber security culture by investing in continuous employee training, awareness programs, and behaviour-based security initiatives that encourage responsibility and compliance. Banks should streamline their organisational structures by establishing well-defined cyber security units, improving coordination between IT, risk management, and operational departments, and adopting more flexible and technology-driven frameworks to respond quickly to evolving threats. Leadership involvement, transparent communication, and regular policy updates are essential to reinforce a security-oriented culture. Additionally, adopting global standards such as the NIST framework, enhancing internal reporting mechanisms, and promoting a culture of accountability can significantly improve cyber resilience in public sector banks.

8. Conclusion

The literature review concludes that cyber security has a significant and transformative impact on the organisational culture and structure of public sector banks. As cyber threats grow more complex, banks are compelled to adopt stronger security frameworks that promote a culture of awareness, compliance, and accountability among employees. At the structural level, the need for efficient risk management has led to the creation of specialised security units, clearer reporting lines, and more technology-integrated organisational models. While challenges such as employee resistance and traditional bureaucratic practices persist, the overall evidence suggests that aligning cultural development with structural changes is essential for building a resilient and secure banking environment. Strengthening both human and organisational capabilities remains crucial for public sector banks to meet emerging cyber security demands.

References

[1] Dhillon, G. (2015). Information Security: Text and Cases. Routledge.
[2] Schein, E. H. (2010). Organizational Culture and Leadership (4th ed.). Jossey-Bass.
[3] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., & McCormac, A. (2017). The influence of organizational culture on information security compliance behaviour. Computers & Security, 68, 35–44.
[4] Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102.
[5] Ifinedo, P. (2014). Information security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management, 51(1), 69–79.
[6] Alshaikh, M. (2020). Developing cybersecurity culture to influence organisational behaviour: A practice perspective. Computers & Security, 98, 102003.
[7] Rao, S. S., & Sahu, G. P. (2013). The role of information security practices in Indian banking sector. International Journal of Advanced Computer Research, 3(3), 154–160.
[8] Reserve Bank of India (RBI). (2017–2022). Cyber Security Framework for Banks and various working papers on cyber security and risk governance. RBI Publications.