Igor Lavrnic [72]
*Academy of Applied Studies of Kosovo and Metohija, Leposavic/Kosovo *.*
Edit Terek [73]
University of Novi Sad, Technical Faculty "Mihajlo Pupin," Zrenjanin/Serbia.

THE ROLE OF ORGANIZATIONAL CULTURE IN SHAPING EMPLOYEE CYBERSECURITY BEHAVIOR

DOI: 10.5937/PIM26260L

Abstract:

Despite the intensive development of research in the field of cyber security, existing approaches still dominantly view security culture through the prism of formal policies, training and technical controls, ignoring the deeper organizational determinants of employee behavior. This paper proposes an original integrative framework - the Four Path Model (FPM) - that operationalizes causal paths from organizational culture to cybersecurity behavior for the first time. The model identifies cybersecurity culture as an emergent property of the broader organizational culture and specifies measurable indicators for each level of culture, addressing the practical challenge of assessing implementation. Unlike previous descriptive models, FPM offers operationalized pathways through which organizations achieve greater compliance, reduce human factor risk, and increase resilience to cyber incidents.

Keywords: *Cyber security culture; organizational culture; employee behavior in cyber security; human factors; cyber risk; organizational resilience; mediation mechanisms; integrative framework*

Introduction

Cyber incidents are primarily caused by the human factor, technical solutions alone cannot neutralize sociotechnical threats [1],[2]. Existing approaches look at safety culture through the prism of policies and training, ignoring the deeper organizational determinants of behavior [1],[2]. The association of culture types with conformity exists in the literature, however, the mechanisms through which this influence is achieved have not been explained so far it is precisely this lack that this paper fills with the identification of mediators [2]. Unlike descriptive frameworks [1],[2],[13], the Four Path Model (FPM) first operationalizes the causal paths from organizational culture to employee behavior through four mechanisms: leadership modeling, organizational trust,

[72] igor.lavrnic@akademijakm.edu.rs, ORCiD: 0009-0009-5333-418X
[73] terek.edit@tfzr.rs, ORCiD: 0000-0003-0013-8141

communication transparency, and normative peer pressure, each with measurable indicators.

The objectives of the work are: (1) synthesis of literature on social-psychological determinants of safety behavior; (2) proposing and operationalizing the Quadruple Pathway Model (FPM) with measurable indicators for each mediating mechanism; (3) development of a diagnostic framework that allows organizations to assess cultural maturity and monitor the progress of interventions. The contribution of the paper is threefold: (1) operationalization of four causal paths from organizational culture to employee behavior in cyber security, with measurable indicators for each; (2) a diagnostic framework for assessing cultural maturity and identifying intervention points; (3) conceptualizing cyber security culture as an emergent property of the broader organizational culture, thus integrating security with organizational development.

1. Research methodology

A qualitative systematic literature synthesis was conducted through Google Scholar, Scopus and Web of Science (2020–2025), with a focus on social-psychological determinants of behavior in the field of cyber security. The criteria for the selection of studies required to include: (a) social-psychological determinants instead of exclusively technical solutions; (b) links between leadership, organizational norms and employee compliance; and (c) theoretical models or empirical evidence on the mediating role of organizational climate. From the 16 selected studies, four mediating mechanisms were identified and integrated into the proposed framework through a thematic synthesis of key concepts including trust, ethical leadership, and social pressure [3],[4],[5],[6].

2. Four Path Model (FPM)

Based on the synthesis of 16 studies (2020–2025), the paper proposes an original integrative framework that explains how organizational culture affects employee behavior in the field of cyber security through four mediating paths, each with an antecedent, process, outcome and measurable indicators. The model is based on a three-level conceptualization [12], operationalized in recent research [12], and integrates the theory of social learning, social bonding, and planned behavior. The basic assumption is that organizational culture does not

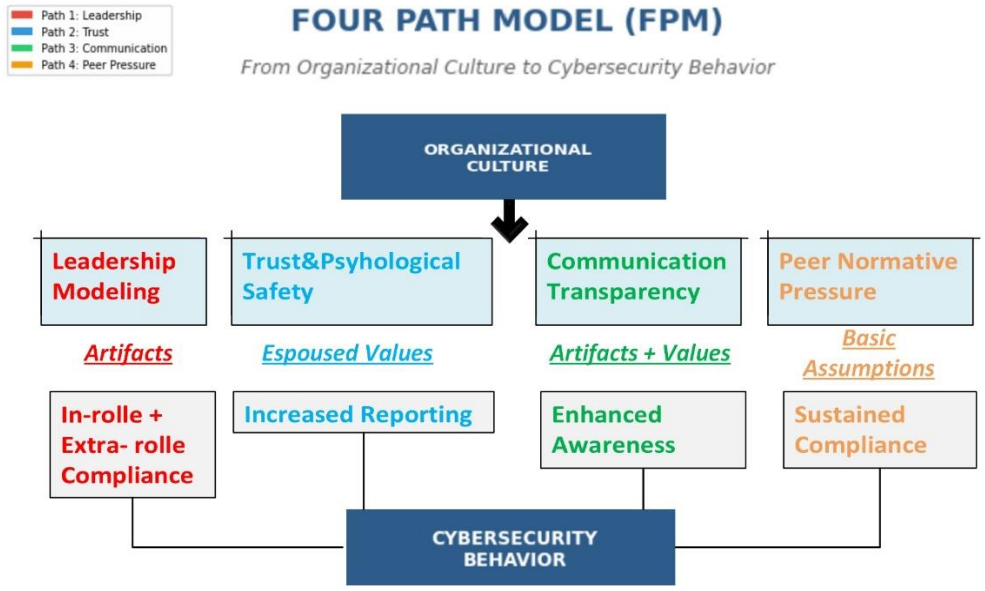
directly determine behavior; its influence is transmitted through four mechanisms at different levels of culture.

Table 1. *Four Path Model (FPM): Path from Organizational Culture to Cyber Security Behavior*

Pathway	Cultural Level	Mediating Mechanism	Behavioral Outcome
1. Leadership Modeling	Artifacts	Employees interpret leadership priorities and security signals [3][4]	In-role compliance + extra-role security citizenship
2. Trust & Psychological Safety	Espoused Values	Trust mediates incident reporting without fear of blame [13]	Increased reporting, reduced concealment of errors
3. Communication Transparency	Artifacts + Values	Shared mental models of threats through open channels [9]	Enhanced awareness, fewer convenience-driven shortcuts
4. Peer Normative Pressure	Basic Assumptions	Normative pressure and organizational commitment [15]	Sustained compliance, reduced neutralization

Unlike previous descriptive models [1],[13], FPM offers operationalized trajectories with antecedents, processes, outcomes, and measurable indicators for each level of culture, allowing practitioners to diagnose which trajectories require intervention and track implementation progress through repeated measurements. This operationalization transforms abstract concepts of culture into measurable constructs.

The Four Path Model (FPM), shown in Picture 1, is an original integrative framework that operationalizes causal pathways from organizational culture to employee cybersecurity behavior through four mediating mechanisms -leadership modeling, trust and psychological safety, communication transparency, and normative peer pressure -where each mechanism operates at a specific level of cultural structure (artifacts, stated values, underlying assumptions) and provides measurable indicators for diagnosing and monitoring implementation.



Picture 1. *The Four Path Model (FPM)*

3. Leadership and SCC

Research highlights the key role of leadership in shaping the organizational safety climate. Ethical leadership has been shown to strengthen information security culture and reduce policy violations [7], while authoritarian-protective (paternalistic) leadership shapes compliance through the perception of sanctions and building a security climate [8]. The concept of a "safety first culture" was introduced, where leadership, communication and continuous learning instill safety as a core value rather than an isolated IT function [9].

Information security culture has been confirmed to mediate between IT infrastructure and organizational performance [10], while human factors -personal convenience and bad habits - have been identified as drivers of unethical behavior such as poor access control, which reduces incident reporting and threatens organizational resilience [11]. Together, these findings show that leadership influence works indirectly through shaping organizational norms and perceptions, integrating safety behavior into a broader cultural context. These findings directly support the First Path of the FPM Model (Leadership Modeling), showing that leadership does not directly influence behavior, but through shaping organizational norms and perceptions [7],[8],[9],[10],[11].

4. Organizational culture and SCC

Organizational culture is key to effective security management, where trust, accountability and open communication directly reduce the risk of threats from employees. Organizational culture has three levels: (1) artifacts (visible practices), (2) stated values, and (3) basic assumptions [12]. Most organizations make the mistake of focusing solely on the surface layers (policies and training), ignoring the deeper layers that fundamentally determine behavior. It has been shown that formal systems alone are not sufficient if safety principles are not adopted as part of the organizational culture [13]. Management, through daily behavior and decisions, imperceptibly shapes the norms and expectations of employees, and it is this example that determines how much safety will actually be respected in practice. It was concluded that cyber security culture is not an independent dimension, but a reflection of a broader culture that determines employees' awareness and reactions to cyber threats [14]. Organizational climate is formed as an operational expression of culture, further influencing social mechanisms that directly shape behavior. The three-level structure of culture [12] and its emergent character [13],[14] form the basis for the Second Path of the FPM model (Trust & Psychological Safety) and the Third Path (Communication Transparency), because values and assumptions determine the degree of trust and openness in the organization.

5. Organizational climate and SCC

The influence of the organizational climate of information security on employee compliance was analyzed through two dimensions: (1) top management's beliefs about the importance of security and (2) the level of organizational control [15]. The results indicate that control systems depend on normative structures, since compliance arises from rational and normative acceptance of the rules, and not only from emotional identification with the company. It has been confirmed that culture, management support and employee attitudes are key factors in compliance [16]. Through the integration of behavioral theories, safety awareness has been identified as a central mechanism.

Organizational climate as an operational expression of culture [15][16] directly shapes the Fourth Path of the FPM model (Normative Peer Pressure), since normative structures generate peer pressure and

organizational commitment, which is a key mechanism for maintaining long-term employee compliance.

6. Mechanisms of influence of organizational culture on safety behavior

The proposed model shows a multi-layered structure of influence on employees' safety behavior. Organizational culture represents the deepest level that shapes values, on the basis of which the organizational climate is formed as an operational expression of culture. Climate further determines social mechanisms such as normative pressure, commitment and commitment that directly dictate the final behavior of the individual (Picture 2).



Picture 2. *Mechanisms of influence of organizational culture on safety behavior.*

7. Discussion and challenges in the implementation of SCC

Despite the integrated approach, the implementation of the model faces two critical challenges. First, the problem of measurability: quantification of artifacts is straightforward, while measuring value internalization requires complex psychometric tools and long-term follow-up. Second, the time discrepancy between the slow evolution of culture and the rapid dynamics of cyber threats. FPM enables organizations to assess cultural maturity, identify weakest paths and track progress through repeated measurements. The key to success lies in a "just culture" that balances protocols with flexibility, encouraging reporting of errors without fear of sanctions, thus reducing harm from inadvertent human error.

8. Conclusion

Technical solutions are not enough without cultural internalization of security. A synthesis of the literature identified four mediating pathways that explain the effectiveness of formal frameworks. The main contribution of the work is the Four Path Model (FPM) which defines the cyber security culture as an emergent property of the wider organizational culture, unlike the previous isolated models [1],[13]. FPM offers operationalized indicators for practical diagnostics and progress monitoring. Management must move from reactive training to active modeling of organizational norms. Future research should validate the FPM through longitudinal studies and cross-cultural comparisons.

REFERENCES

[1] Sutton, A. and Thompson, L. (2025). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. Computers & Security, 148, 104110. doi: 10.1016/j.cose.2024.104110.

[2] Karlsson, M., Karlsson, F., Åström, J. and Denk, T. (2022). The effect of perceived organizational culture on employees' information security compliance. Information & Computer Security, 30(3), 382–401. doi: 10.1108/ICS-06-2021-0073.

[3] Tejay, G.P.S. and Winkfield, M. (2025). Does Leadership Approach Matter? Examining Behavioral Influences of Leaders on Employees' Information Security Compliance. Information Systems Frontiers. doi: 10.1007/s10796-025-10592-4.

[4] Almeida, M.C., Yoshikuni, A.C., Dwivedi, R. and Larieira, C.L.C. (2022). Do Leadership Styles Influence Employee Information Systems Security Intention? A Study of the Banking Industry. Global Journal of Flexible Systems Management, 23(4), 535–550. doi: 10.1007/s40171-022-00320-1.

[5] Alkhazi, B., Alshaikh, M., Alkhezi, S. and Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. IEEE Access, 10, 132132–132143. doi: 10.1109/ACCESS.2022.3230286.

[6] Sulaiman, N.S., Fauzi, M.A., Wider, W., Rajadurai, J., Hussain, S. and Harun, S.A. (2022). Cyber-Information Security Compliance and Violation Behavior in Organizations: A Systematic Review. Social Sciences, 11(9), 386. doi: 10.3390/socsci11090386.

[7] Zhang, J., Li, Y. and Wang, X. (2023). Ethical Leadership and Information Security Compliance: The Mediating Role of Security Culture. Journal of Business Ethics, 185(2), 421–438. doi: 10.1007/s10551-022-05123-4.

[8] Zhu, T., Chen, H. and Liu, W. (2024). Paternalistic Leadership and Employee Security Behavior: A Multi-Level Analysis. Information & Management, 61(3), 104012. doi: 10.1016/j.im.2023.104012.

[9] Willie, M.M. (2023). The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture. Journal of Research and Innovation in Technology (JoRIT), 2(16), 180. doi: 10.57017/jorit.v2.2(4).05.

[10] Hassan, Y. et al. (2025). Exploring the Mediating Role of Information Security Culture in Enhancing Sustainable Practices Through Integrated Systems Infrastructure. Sustainability, 17(2), 687. doi: 10.3390/su17020687.

[11] Chu, A.M.Y. and So, M.K.P. (2020). Organizational Information Security Management for Sustainable Information Systems: An Unethical Employee Information Security Behavior Perspective. Sustainability, 12(8), 3163. doi: 10.3390/su12083163.

[12] Adamu, M.A., Niemimaa, M.I. and Spagnoletti, P. (2025). Towards a Three-Tiered Framework for Fostering Organizational Cybersecurity Culture. In M. Themistocleous et al. (Eds.), Lecture Notes in Business Information Processing, 536 (pp. 313–324). Cham: Springer Nature Switzerland. doi: 10.1007/978-3-031-81325-2_22.

[13] Da Veiga, A., Astakhova, L.V., Botha, A. and Herselman, M. (2020). Defining organizational information security culture—Perspectives from academia and industry. Computers & Security, 92, 101713. doi: 10.1016/j.cose.2020.101713.

[14] Xue, D., Chen, L. and Zhang, Y. (2023). Cybersecurity Culture as Organizational Culture Reflection: A Multi-Industry Study. Computers & Security, 132, 103356. doi: 10.1016/j.cose.2023.103356.

[15] Dong, F., Zhang, S., Zhu, J. and Sun, J. (2021). The Impact of Information Security Climate on Employee Compliance Behavior: A Normative Perspective. International Journal of Information Management, 59, 102356. doi: 10.1016/j.ijinfomgt.2021.102356.

[16] Vicente, A., Díaz-Marcos, L., Aguado-Tevar, O. and García de Blanes-Sebastián, M. (2025). Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity. Future Business Journal. doi: 10.1186/s43093-025-00452-7.