TPM Vol. 32, No. S2, 2025
ISSN: 1972-6325
https://www.tpmap.org/

Open Access

EXPLORING IMPLICIT BIAS IN ENGINEERING SECURITY TOOL ADOPTION WITH TRAINING INSIGHTS FOR HR AND IT

PRACHI GURUDIWAN
ASSISTANT PROFESSOR, KALINGA UNIVERSITY, RAIPUR, INDIA.
EMAIL: ku.prachigurudiwan@kalingauniversity.ac.in, ORCID ID:0009-0008-0150-5250

DR. SHYAM MAURYA
ASSISTANT PROFESSOR, KALINGA UNIVERSITY, RAIPUR, INDIA.
EMAIL: ku.shyammaurya@kalingauniversity.ac.in ORCID: 0009-0006-3442-8621

GAJENDRA SINGH NEGI
ASSISTANT PROFESSOR, NEW DELHI INSTITUTE OF MANAGEMENT, NEW DELHI, INDIA
EMAIL: gajendra.negi@ndimdelhi.org, HTTPS://ORCID.ORG/0009-0007-6916-5291

Abstract
Engineering teams often do not choose to adopt new security tools for technical reasons; rather, they often choose not to because of implicit psychological biases that lead to cognitive distortions that affect assessments of risk and trust. This paper investigates the cognitive variables that affect engineers' trust and risk beliefs when adopting tools; these variables include overconfidence, ambiguity aversion, familiarity bias, biases toward the status quo, and perceived effort. Using psychometric models, such as TPMAP, we have noted that the confusion surrounding trust calibration, role beliefs, and unconscious processing produces persistent patterns of resistance that have not been considered in traditional models of technology adoption. Developers, DevOps, and Security Engineers exhibit different trust-risk profiles, dependent on individual cognitive propensities and social framing factors - namely, their organizational framing of their safety-critical role. Resistance to new tools, especially when tool adoption is framed as compliance mandates rather than aims of enabling one's security capability, can elicit considerable emotional resistance - and reasonable moralizing, especially when the tools involve surveillance. In response to these challenges, we propose a common HR-IT training plan starting with onboarding biases, gradualisation (scenarios), and reinforcements using trust dashboards - to realign people's biases, reduce 'cognitive friction', and to foster psychologically intelligent security cultures. Our research calls for the exploration of cognitive load UI, emotional telemetry, and personalized training pathways. In this regard, we put forward that researchers should embrace a human-centered approach to technology adoption - rather than a technology-centered one. This type of better consideration of the social implications and responsibilities of technology in the security domain has not received enough critical review.

Keywords: Implicit Bias, Cognitive Framing, Security Tool Adoption, Trust Perception, Engineering Psychology, HR Training, Psychometric Profiling

INTRODUCTION

In today's engineering contexts, we know that adopting security tools is not just a technical action; it is also fundamentally a decision shaped by human psychology. Security risks are often accepted because risk management through advanced security tools is available to the engineer and manager; however, they often resist the integration of new security tools. This resistance is often dictated by unconscious cognitive biases like overconfidence in their practices, distrust in using something automated, and avoidance due to perceived role boundaries. Often these biases exist in an unconscious place, which will drive attitudes and behaviours in subtle and powerful ways. Traditional models for the adoption of technology often centre on usability and performance, and affordability, but often ignore the psychological frame of reference barriers that arise from how we think as individuals in a group culture [6]. Our unconscious processing, shaped by our past experiences and our identity as we participate in our social roles, also shapes how the engineer will see risk and assess the optimallyvaluable security intervention and behaviour. In addition to cognitive biases, the organizational norms and expectations (like being quick to deliver or not respecting the instructions of compliance) can also maintain these biases [1]. After all, the challenge of seated biases in human behaviour can lead to effective and sustainable security behaviours and practices in teams of technical expertise [4].

I. Cognitive Anchors in Tool Adoption: A Psychometric Perspective

It is common to assume that engineering decisions are rational and grounded in evidence. However, engineering decisions are potentially subjected to the influences of cognitive anchors or mental shortcuts and biases, which are key elements in how we evaluate or adopt tools. One issue is cognitive load. When engineers work in constrained time frames, have to juggle many projects or have many related tasks on their plate, they are distant from exploring new tools because any additional mental capacity is going to risk efficiency [15]. Furthermore, perceived effort compared to return on investment is critical. Security tools are often ignored if they appear lean on effort, if they seem intrusive, or if their return appears uncertain, and yet the positive outcomes may remain unchanged regardless of the perceived effort involved [5].

Familiarity bias also plays its part in adoption, when engineers gravitate toward tools and practices that they have utilized before or those that appear to have lesseffect than the effects of the alternatives. The similarly associated status quo bias, where systems and workflows are maintained not due to superiority or optimum function, but because the steps are known and deemed safe and fulfilling [12]. These biases often happen implicitly; however, a researcher can quantitatively investigate the extent to which engineering biases are influencing a tool evaluation process using psychometric tools such as TPMAP-style trust metrics, which look at trust thresholds, orientation to risk, or decision to default. The research model operationally defines how engineers internally weigh new tools and their considerations, norms, and prior experiences influence their evaluation of the utility to adopt [14].

Table 1: Key Cognitive Biases and Their Effects on Security Tool Adoption

Bias Type	Description	Effect on Tool Adoption
Cognitive Load	Mental strain from multitasking or complexity overload	Engineers avoid engaging with tools that demand extra effort
Familiarity Bias	Preference for known tools and workflows	Resistance to exploring new or unfamiliar security solutions
Status Quo Bias	Inertia toward current practices, fear of disruption	Continuation of outdated or insecure habits
Perceived Effort	Misjudgment of the cost-benefit ratio of tool usage	Underutilization of effective tools due to perceived burden
Overconfidence	Belief in one's security practices as sufficient	Dismissal of additional tools as unnecessary

Table presents the primary cognitive biases that affect engineers' perceptions and uptake of security tools within organizations [8]. Each bias operates below the radar (cognitively) and contributes to resistance in various ways. Take cognitive load, for example, and it prevents uptake of a tool altogether if engineers are cognitively overloaded, or familiarity bias induces reliance on existing systems, even if they are obsolete. Status quo bias strengthens workflows that already exist,not to yield any openness to change, and perceived effort alters judgements about adopting tools, where the cost in effort seems higher than the benefits. Overconfidence distorts the belief that existing security measures are adequate or personal disposal tracing is enough, which reduces the desire for any additional security measures. The biases are categorized to distinguish the behaviours and map the consequential behavioural phenomenon [3]. The table serves as a starting point to develop targeted interventions, which alignwith the paper's contention that the resistance to security tools has less to do with the functional assets of the tools and more about how they are framed, trusted, and cognitively understood. The work helps to highlight the need for informed psychometric learning and role-focused strategies where applicable [7].

Psychological inertia, which is rooted in remembering early failures, mimicking peer behavior, and stereotypes (e.g., seeing security as a job of another group), results in a constrained set of responses where we cannot fix the psychological constraints in a single training session. Recognizing these cognitive patterns is essential to designing interventions to reduce resistance and open possibilities for security engagement with innovations [13].

Trust, Risk Perception, and Framing Organizational Roles

The importance of calibrated trust or calibrated belief, which is outlined in some TPMAP frameworks, is essential to understanding how engineers interact with security tools. Trust in a tool is a reflection of a user's alignment with a tool's trust, not too high or it may invite blind trust, not too low or it may lead to rejection. Different engineering roles elicit different trust-risk profiles or interactions. Developers may weigh speed and functionality rather highly and see security tools as impeding innovation. Security Engineers appear to weigh trust in a tool either highly with rigorous delineation of controls or structured enforcement. DevOps teams that find themselves between deployment and reliability seem to be weighing performance and protection, and may have the least definitive trust levels depending on the context.

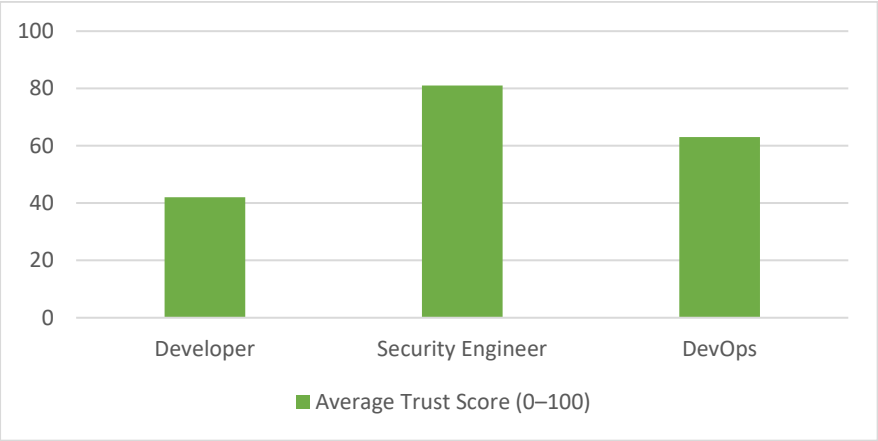

Figure 1: Comparative Trust Scores Across Engineering Roles

Figure 1 shows role-based differences in their average trust scores for new security tools in the psychometric profiles that were designed using TPMAP-type trust calibration metrics. These data illustrate how security engineers report trust levels that are higher because the tools are consistent with their core role, as devs have lower trust levels, habitually justified by peer disruption and autonomy behavior. The DevOps personnel had mid-range trust scores in-between engineers and developers because of their balancing act of performance and security. Rationale mapping in training approaches and developing framing efficacy are required, as the perception of trust is non-uniform across roles within the technical theater.

These views are heavily influenced by framing an organizational role. When a tool is introduced as an imposition for compliance, it often engenders psychological resistance or rejection from employees (especially when they feel their autonomy is at stake). Conversely, using the same tool as a resource for empowerment, such as increasing control, diminishing error, or contributing to the team's goals, tends to create a more positive reception.

Moreover, perceived surveillance plays a central role in emotional resistance. Engineers who think that security tools could be used to gauge their performance or to oversee their work with punishments in mind will very likely create some disengagement or covert non-compliance (or whatever you want to call it). This emotional response, which is grounded in the erosion of trust, can derail even some of the most thoughtfully designed implementations. If you can acknowledge the reality of these dynamics and alter your approach to communication, you might foster new relationships or constructive engagement. Calibrated recognition and trust-buildinggoing slow and being transparent, creating user feedback loops, onboarding role-based users, can create the opportunity to migrate organizational framing from resisting to aligning.

Training Interventions: A hybrid HR and IT-based de-biasing model

As we have shown, moving more than just addressing implicit bias in the adoption of engineering tools requires more than observable proficiency in upskilling and technical adoption; we are unpacking a class of psychological interventions intended to modify how engineers identify, judge, and interact with security tools.

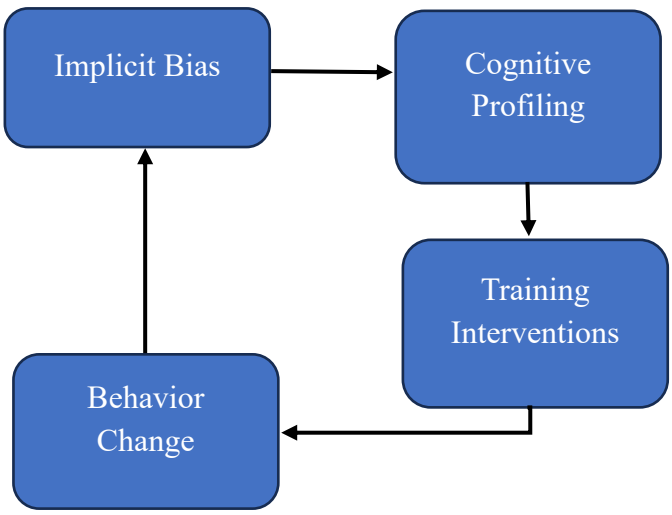

Figure 2: Psychological Enablement Flowchart for Security Tool Adoption

Figure 2demonstrates a cyclicality of implicit bias, cognitive profiling, intervention-training-objects, and behaviour change as it relates to engineers' adoption of security tools. The process begins with the identification of unconscious biases like over-confidence (cockiness-level) and familiarity biases, which are then subject to psychometric profiling to be able to identify and understand certain cognitive mediums based on role; Reasoning and judgement platform | capabilities. These are then sent to HR and IT to build training intervention strategies |

angles for pilots that include onboarding | testing | micro learning bits, and feedback responses for intervention training tools. The behaviour change responses are targeted to change engineer biases and make them work with security tools with more open trust, calibrated engagement. That behaviour change interferes with the biases, thus completing feedback, an improvement was facilitated for future modelling.

This undertaking is not possible without the collaboration of Human Resources and Information Technology as engaged partners using psychometric insight and learning design [2].On the Human Resource side of the ledger, we can embed bias-awareness modes within onboarding processes that are built upon psychometric profiles [9]. Bias-awareness modules will help new hires understand cognitive dispositions like overconfidence, status quo bias, or aversion to risk. Using instruments like TPMAP, individuals have the benefit of tailored feedback about their cognitive profile, highlighting how this might affect security behaviours related to tool use. This serves to give new hires an enhanced awareness of themselves and helps to normalize the presence of bias in technical decision-making.On the Information Technology side, they can use micro-learning models – very small, scenario-based modules in which the users engage in contextual dilemmas that involve tool use, trust in automation, or adherence to policy, and so on and on. These simple scenarios press the users to think about why they made, in a circumstance of uncertainty or time pressure, a particular decision in situ. By revealing their reasoning, in openings such as this,lie hidden biases. If we apply this type of learning over many interactions, it is hoped we will desensitize automatic responses and move towards more adaptive thinking.There is potential for shared dashboards to complement those tools and provide transparent trust metrics, allowing engineers to view and reflect on their practice with, and in, the tools against the baseline of team norms or security objectives; avoiding any surveillance optics, and directed more towards team-view, team-level insight, team-growth tracking, and behavioral feedback loops.Other tools may be the addition of reflective prompts in workflows (e.g., “You missed that security check, why?”), peer-to-peer post-action debriefs, and development or DevOps or security-specific content with targeted personas. Altogether, those can help create a psychologically intelligent training ecosystem, conducive to lasting behavioral change, without forfeiting autonomy and experience [11].

CONCLUSION

This study has shown that resistance to the adoption of security tools in engineering contexts is not only due to issues of technological compatibility or usability, but rather it is based on deeper-seated psychological dimensions. Implicit biases, trust misalignment, and role-based cognitive framing processes significantly shape the way that engineers evaluate and engage with security interventions, and recognizing these patterns shifts our attention to areas further beneath the surface of compliance; specifically, the cognitive architecture of decision making. In the future, organizations will have to continue addressing the nature of psychometric calibration, which will permit more precise definitions of engineers' trust thresholds, risk propensities, and triggers for bias across engineering personas. This work would include the need for adaptive training programs that do not attempt to provide standardized instruction, but rather the psychologically informed delivery of contextually specific content. Most importantly, HR and IT units must work together in the co-design of cognitive mapping, ultimately facilitating onboarding, feedback, and real-time insight into behavioral change [10]. Future studies should also focus on developing cognitive load-sensitive interfaces, experiential telemetry systems that find friction points, and tailored learning paths that are responsive to individual cognitive styles. Only through psychologically-informed thinking and practice in the security adoption lifecycle can an organization achieve technical resilience and human alignment.

REFERENCES

[1] Usikalu, M., & Okafor, E. (2025). Strategic Innovation Models for Enhancing Organizational Agility in the Knowledge Economy. *International Academic Journal of Innovative Research*, *12*(1), 8–13. https://doi.org/10.71086/IAJIR/V12I1/IAJIR1202

[2] Pal, A., & Chhabra, D. (2025). Federated Learning for Healthcare Privacy-Preserved Artificial Intelligence in Distributed Systems. *International Academic Journal of Science and Engineering*, *12*(1), 7–11. https://doi.org/10.71086/IAJSE/V12I1/IAJSE1202

[3] Velliangiri, A. (2025). Bio-inspired vortex control mechanisms for drag reduction in high-speed submerged bodies: A CFD and experimental study. Advances in Mechanical Engineering and Applications, 1(1), 11–22.

[4] Seyedan, S. A. (2017). A Study of the Relationship between Personality Traits and Internet Addiction among Secondary School Male Students in Torbat Heydarieh. *International Academic Journal of Social Sciences*, *4*(2), 73–83.

[5] Tirkey, S., Mishra, D., & Mahalik, D. K. (2020). A Study on ‘Why Outsourcing in Health Care’ by Friedman: Two-way Analysis of Variance Method. *International Academic Journal of Organizational Behavior and Human Resource Management*, *7*(1), 01–08. https://doi.org/10.9756/IAJOBHRM/V7I1/IAJOBHRM0701

[6] Uvarajan, K. P. (2025). Integrating adapted yoga into sports-based occupational therapy for children with autism. Journal of Yoga, Sports, and Health Sciences, 1(1), 31–38.
[7] Vincentelli, B., & Schaumont, K. R. (2025). A review of security protocols for embedded systems in critical infrastructure. SCCTS Journal of Embedded Systems Design and Applications, 2(1), 1–11.
[8] Kavitha, M. (2025). Breaking the silicon ceiling: A comparative analysis of women's leadership and participation in AI startups across global innovation hubs. Journal of Women, Innovation, and Technological Empowerment, 1(1), 1–6.
[9] Mitra, A., & Shah, K. (2024). Bridging the Digital Divide: Affordable Connectivity for Quality Education in Rural Communities. *International Journal of SDGs Prospects and Breakthroughs*, *2*(1), 10-12.
[10] Poornimadarshini, S. (2024). Comparative techno-economic assessment of hybrid renewable microgrids in urban net-zero models. Journal of Smart Infrastructure and Environmental Sustainability, 1(1), 44–51.
[11] Kapoor, P., & Malhotra, R. (2025). Zero Trust Architecture for Enhanced Cybersecurity. In *Essentials in Cyber Defence* (pp. 56-73). Periodic Series in Multidisciplinary Studies.
[12] Ansari, H., & Parmar, J. (2024). Tracing Human Evolution through Ancient DNA: Insights from Paleogenomic Studies. *Progression Journal of Human Demography and Anthropology*, *2*(3), 13-16.
[13] Ferreira, M., Pereira, J., & Costa, A. (2024). The Hidden Link between Quality Management and Digital Success: A Fortune 500 Case Study. National Journal of Quality, Innovation, and Business Excellence, 1(2), 40-50.
[14] Kapoor, A., & Gupta, R. (2023). Development of a Real-Time Multilingual Medical Terminology Translator for Emergency Settings. *Global Journal of Medical Terminology Research and Informatics*, *1*(1), 16-19.
[15] Shimazu, S. (2024). Intelligent, Sustainable Supply Chain Management: A Configurational Strategy to Improve Ecological Sustainability through Digitization. *Global Perspectives in Management*, *2*(3), 44-53.
[16] Hakkaraki, V. (2023). A Bibliometric Analysis of Journal of Scientometric Research Based on Dimensions Database. Indian Journal of Information Sources and Services, 13(1), 26–31. https://doi.org/10.51983/ijiss-2023.13.1.3486
[17] Said, N. M. M., Ali, S. M., Shaik, N., Begum, K. M. J., Shaban, A. A. A. E., & Samuel, B. E. (2024). Analysis of Internet of Things to Enhance Security Using an Artificial Intelligence-based Algorithm. Journal of Internet Services and Information Security, 14(4), 590-604. https://doi.org/10.58346/JISIS.2024.I4.037
[18] Smith, J., Harris, J., & Martin, C. (2024). Why UN's SDG Goals Are Missing their Targets. Journal of Tourism, Culture, and Management Studies, 1(2), 38-49.
[19] Vasilievich, S. P., Shapovalov, V., Vasin, A., Grinevich, V. B., & Semenov, K. (2025). Evaluation of the Effectiveness of an AI-Based Telemedicine System for Remote Screening of Chronic Disease Risks. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 16(1), 217-229. https://doi.org/10.58346/JOWUA.2025.I1.013
[20] Dmytrenko, O., Lutsenko, T., Dmytrenko, A., & Bespalova, O. (2024). Assessment of Efficiency and Safety of Phytocomposition with Prostate-Protective Properties in the form of Rectal Suppositories. Natural and Engineering Sciences, 9(2), 407-425. https://doi.org/10.28978/nesciences.1465276