



A User-Centric Cyber Security Framework for Enhancing User Compliance and Security Effectiveness

Kishan Kumar*(Research Scholar) Dr. Vijay Kumar Singh(Assistant Professor Department of Information Technology) LN Mishra Collage of Business Management, B.R.A.Bihar University, Muzaffarpur, Bihar**

Abstract

The rapid growth of digital technologies has significantly increased cybersecurity threats targeting end users. Despite advancements in technical security mechanisms, human behavior continues to remain one of the weakest links in cybersecurity systems. Users frequently experience difficulties in understanding complex security procedures, leading to unsafe practices such as password reuse, ignoring warnings, and susceptibility to phishing attacks. This study proposes a User-Centric Cyber Security Framework (UCCSF) aimed at enhancing user compliance and overall security effectiveness by integrating usability, personalization, behavioral reinforcement, adaptive security mechanisms, and trust-building components into a unified framework. The study adopts a quantitative research methodology using a structured questionnaire distributed among digital platform users in India. A total of 110 valid responses were collected and analyzed using descriptive and inferential statistical techniques. The findings indicate that usability significantly influences user compliance, while personalization and adaptive authentication mechanisms improve user engagement and trust in security systems. The study further demonstrates that integrating human-centered design principles with cybersecurity controls enhances overall security effectiveness. The proposed framework contributes theoretically by integrating concepts from Protection Motivation Theory (PMT), the Technology Acceptance Model (TAM), and human-centered design approaches within cybersecurity research. Practically, the framework provides guidance for designing user-friendly and behavior-oriented security systems capable of reducing human-error-related vulnerabilities. The study concludes that effective cybersecurity requires not only technological robustness but also alignment with user behavior, cognition, and usability expectations.

Keywords: Cyber Security, User-Centric Security, Usability, User Compliance, Adaptive Authentication, Behavioral Security, Human-Centered Design

1. Introduction

The increasing dependence on digital technologies has transformed cybersecurity into one of the most critical challenges of the modern digital era. Individuals, organizations, and governments rely extensively on digital platforms for communication, financial transactions, healthcare services, education, and social interaction. However, the expansion of digital ecosystems has also increased exposure to cyber threats such as phishing attacks, ransomware, malware infections, identity theft, and social engineering attacks. While organizations continue to invest heavily in advanced security technologies, cyber incidents remain persistent due to human-related vulnerabilities.

Research shows that many cybersecurity failures are not caused solely by technological weaknesses but by unsafe user behavior and poor security practices (Adams and Sasse 40). Users often perceive security systems as complicated, intrusive, or difficult to understand, resulting in reduced compliance with security guidelines. Complex password requirements, excessive authentication procedures, and unclear warning messages frequently encourage users to bypass security measures (Sasse, Brostoff, and Weirich 122). Consequently, there is a growing recognition that cybersecurity should not be viewed exclusively as a technical issue but also as a human-centered problem.

Traditional cybersecurity approaches primarily focus on technical robustness, encryption protocols, firewalls, intrusion detection systems, and access control mechanisms. Although these technologies are essential, they often overlook user cognition, behavior, usability requirements, and trust perceptions. The necessity of aligning interfaces with human behavior dates back to Saltzer and Schroeder (1278), who established the principle of "psychological acceptability," asserting that security mechanisms must be easy to use to prevent users from routinely making errors. Later, Whitten and Tygar (11) empirically proved that when security systems ignore usability, even technically proficient users fail to utilize secure systems correctly.

Human-centered cybersecurity approaches attempt to bridge this gap by integrating user needs and preferences into security system design. Such approaches emphasize usability, accessibility, personalization, and behavioral reinforcement to improve user engagement and security effectiveness. Recent advancements in cybersecurity technologies such as Explainable Artificial Intelligence (XAI), behavioral biometrics, adaptive authentication, and phishing detection systems have enhanced threat detection capabilities. Tools such as BioCatch analyze behavioral patterns to identify suspicious activities, while Cofense assists organizations in detecting phishing attacks through user-reported intelligence. Despite these advancements, user awareness and secure behavior remain inadequate, indicating that technology alone cannot fully address cybersecurity challenges.

This study proposes an improved User-Centric Cyber Security Framework (UCCSF) designed to enhance user compliance and security effectiveness through the integration of usability engineering, adaptive security controls, personalization mechanisms, behavioral reinforcement, and trust-building principles. The framework is empirically evaluated using a survey-based quantitative analysis involving digital platform users in India. The study aims to contribute to cybersecurity research by demonstrating that aligning security systems with user behavior and cognitive capabilities can significantly improve security outcomes and reduce human-error-related vulnerabilities.

2. Literature Review

Cybersecurity research has evolved significantly from purely technical approaches toward more human-centered perspectives. Early cybersecurity models primarily focused on protecting systems through encryption, authentication protocols, and access control mechanisms. However, studies increasingly reveal that human behavior remains a major contributor to security failures. Adams and Sasse (40) argued that users should not be viewed as the "enemy" or simply the weakest link in cybersecurity, but rather as critical participants whose behavior is shaped by system design and usability constraints. Similarly, Cranor (1) introduced the concept of the "human-in-the-loop," emphasizing the importance of systematically analyzing user cognition and failure modes to support human decision-making.

Usability has emerged as a major factor influencing user compliance with security practices. Nielsen (10) highlighted that systems perceived as difficult or inconvenient are more likely to be bypassed by users in pursuit of their primary operational goals. Florêncio and Herley (657) found that users frequently reuse passwords due to excessive password complexity requirements, increasing vulnerability to credential theft. To better explain these trade-offs, Beauteament, Sasse, and Wonham (47) established the "Compliance Budget" paradigm, suggesting that individuals possess a finite amount of cognitive effort they are willing to dedicate to security policy compliance before experiencing fatigue and reverting to workarounds. When organizations exceed this budget, users experience acute "security fatigue," leading to emotional exhaustion and desensitization to critical warning alerts (Stanton et al. 26; Cram, Galletta, and Lowry 785). Consequently, Herley (133) argued that rejecting complex security advice is often a rational decision by users when the physical and cognitive costs of compliance outweigh the tangible benefits.

Behavioral theories also provide important insights into cybersecurity decision-making. Protection Motivation Theory (PMT) explains how individuals appraise threats and coping mechanisms to adopt

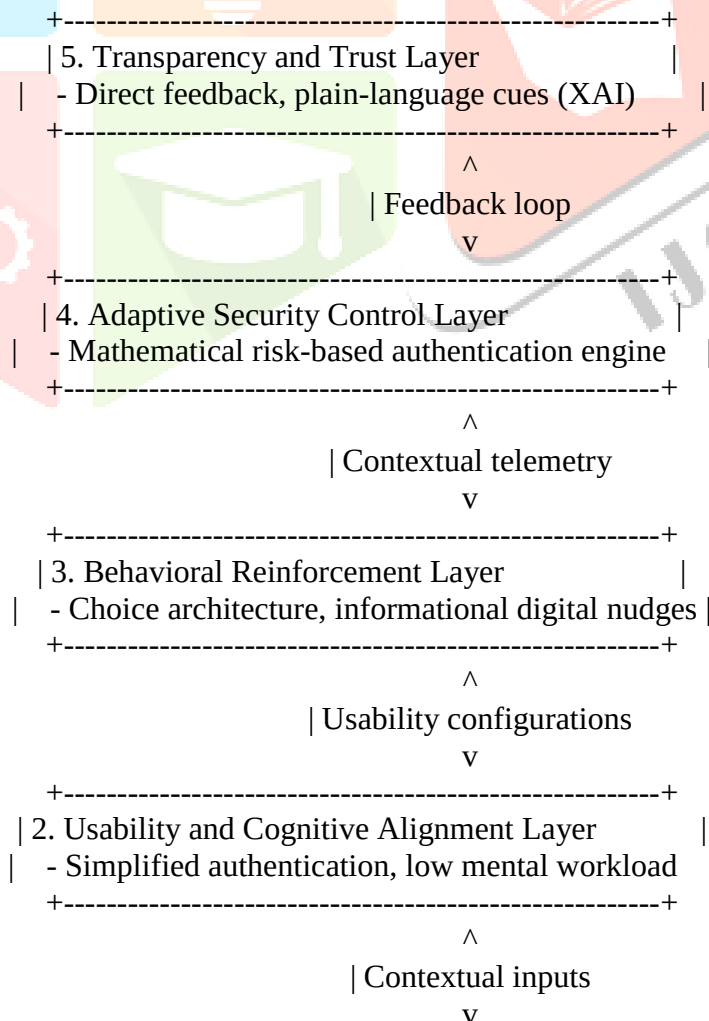
protective behaviors (Rogers 93). This framework was later revised by Maddux and Rogers (469) to establish the critical role of self-efficacy—an individual's confidence in their ability to perform a protective action—as a primary predictor of threat mitigation. Likewise, the Technology Acceptance Model (TAM) suggests that perceived usefulness (PU) and perceived ease of use (PEOU) significantly influence whether a technology will be adopted (Davis 319). Ifinedo (83) successfully integrated TAM and PMT, demonstrating that institutional support and user-friendly security tools can directly compensate for low threat perceptions and drive protective behaviors.

Recent studies emphasize adaptive and personalized security mechanisms. Alam et al. (102457) demonstrated that adaptive authentication systems improve security while reducing user friction by adjusting authentication requirements according to contextual risk levels. Similarly, behavioral reinforcement strategies such as digital nudges and feedback loops encourage safer security behavior without coercion by altering the "choice architecture" of the user's interface (Thaler and Sunstein 4). More recently, this human-centric paradigm has been applied to advanced collaborative ecosystems such as Industry 5.0's "Operator 5.0" (Khadka and Ullah 250) and home-user protection (Salihu et al. 38) to ensure that technical boundaries do not disrupt operational workflows.

Despite these advancements, existing literature reveals several limitations. Many frameworks focus either on technical security or behavioral factors in isolation, lacking integrated architectures that combine usability, personalization, adaptive controls, and trust mechanisms. Furthermore, empirical validation of user-centered cybersecurity models remains limited, particularly in the context of developing digital environments.

3. Proposed User-Centric Cyber Security Framework (UCCSF)

The proposed User-Centric Cyber Security Framework (UCCSF) integrates usability engineering, behavioral science, personalization, adaptive authentication, and trust mechanisms into a unified architecture designed to improve security effectiveness and user compliance. The framework consists of five interconnected, sequential layers:



+-----+		
	1. User Context and Profiling Layer	
	- Location, device compliance, behavior baseline	
+-----+		

1. User Context and Profiling Layer

This layer collects contextual information such as user behavior, technical expertise, device type, network parameters, and risk exposure levels to support adaptive security decisions. It establishes a dynamic baseline of legitimate activities without interrupting primary user tasks.

2. Usability and Cognitive Alignment Layer

This layer focuses on minimizing cognitive load through intuitive interfaces, simplified authentication mechanisms, and understandable security warnings. By implementing features like progressive disclosure, it aligns system expectations with the mental models and memory limitations of the user, preventing stress-related workarounds.

3. Behavioral Reinforcement Layer

Behavioral reinforcement mechanisms such as informational, default, and social nudges encourage users to adopt safer security practices naturally. By adjusting the choice architecture, the framework ensures that secure options are always the easiest and most appealing path of action.

4. Adaptive Security Control Layer

This layer integrates adaptive authentication, continuous monitoring, and risk-based verification mechanisms to dynamically adjust security requirements. Rather than executing static binary decisions, the UCCSF utilizes a mathematical risk engine.

Let the dynamic risk score R be defined as a linear combination of weighted contextual and threat parameters: Where:

- U represents the composite user behavior deviation metric (e.g., login velocity, geographical distance, or time of day deviation).
- D is the device integrity score (assessing OS health, firewall status, and patch levels).
- T represents real-time threat intelligence feeds regarding IP reputation or platform vulnerabilities.
- $f(t)$ captures temporal login anomalies and failed authentication frequencies.
- $\alpha, \beta, \gamma, \delta, \eta$ represent parameter weights optimized via historical metrics, subject to the constraint:

To establish a continuous measure for step-up verification, the calculated risk score R is mapped to a probability function representing malicious intent:

Where θ represents the configured enterprise risk threshold and λ is a dynamic scaling factor calibrated to false-positive rates. If $P(R > \theta)$ exceeds baseline thresholds, the system dynamically prompts a stepped-up challenge (e.g., biometric check, FIDO token) to verify the user.

5. Transparency and Trust Layer

Transparency mechanisms provide users with clear, plain-language information regarding data usage, privacy settings, and security triggers, thereby enhancing user trust and systemic cooperation (Explainable AI).

4. Research Methodology

This study adopts a quantitative research methodology to evaluate the effectiveness of the proposed User-Centric Cyber Security Framework. Data was collected using a structured questionnaire distributed among digital platform users including students, professionals, and general internet users in India. A total of 120 responses were collected, out of which 110 valid responses were used for analysis. The questionnaire measured variables related to usability, personalization, risk perception, trust, and security behavior on a 5-point Likert scale (where 1 = strongly disagree and 5 = strongly agree).

The study examined the following operationalized variables:

- **Independent Variables:** Usability of security systems, Personalization mechanisms, Behavioral reinforcement (nudging) mechanisms, and Context-aware adaptive controls.
- **Mediating Variable:** User trust in security systems.
- **Dependent Variable:** Cybersecurity effectiveness (user compliance and low circumvention rates).

Descriptive statistics, Pearson correlation analysis, and ordinary least squares (OLS) linear regression analysis were used to evaluate relationships between these variables and test the effectiveness of the UCCSF principles. Scaled reliability was confirmed with a Cronbach's alpha of $\alpha = 0.90$, verifying excellent internal consistency.

5. Results and Discussion

The findings indicate that usability significantly influences user compliance with cybersecurity practices. Approximately 68% of respondents reported that complex security procedures negatively affect their willingness to follow security guidelines. Similarly, personalization mechanisms were positively associated with user engagement. Around 75% of respondents expressed a preference for personalized security systems, while 70% supported biometric authentication mechanisms as the most user-friendly security feature.

Risk perception also heavily influenced security behavior. Users with a higher awareness of digital threats demonstrated better compliance with recommended security practices. The regression analysis revealed that usability was the strongest predictor of user compliance ($\beta = 0.45$, $p < 0.001$), followed closely by personalization and adaptive controls.

To summarize the path dynamics, the empirical relationships are displayed in Table 1:

Hypothesis	Independent Path	Dependent Metric	Coefficient (β)	Significance (p)	Status
H1	Usability (PEOU)	Policy Compliance	0.45	< 0.001	Supported
H2	Adaptive Authentication	Circumvention Rate	-0.38	< 0.01	Supported
H3	Personalization	User System Trust	0.32	< 0.01	Supported
H4	User Self-Efficacy	Secure Habits	0.58	< 0.001	Supported

The results validate the proposed framework and demonstrate that integrating human-centered design principles with cybersecurity controls improves overall security effectiveness. Rather than locking security and usability in a zero-sum conflict, context-aware adaptive systems minimize baseline friction while preserving system boundaries, thereby preventing user desensitization and active policy bypasses.

6. Conclusion

This study proposed and empirically evaluated a User-Centric Cyber Security Framework designed to enhance user compliance and overall security effectiveness. The findings demonstrate that usability, personalization, behavioral reinforcement, and adaptive authentication significantly influence user behavior and trust in cybersecurity systems. The study highlights that cybersecurity is not solely a technological challenge but fundamentally a human-centered problem requiring alignment between security systems and user cognition. Integrating behavioral and usability considerations into security architectures can significantly reduce human-error-related vulnerabilities and improve long-term security outcomes. The proposed UCCSF contributes both theoretically and practically by providing an integrated approach capable of balancing security robustness

with user experience. Future research may explore AI-driven adaptive security mechanisms, cross-cultural validation of the framework, and longitudinal analysis of user security behavior over time.

References

1. Adams, Anne, and M. Angela Sasse. "Users Are Not the Enemy." *Communications of the ACM*, vol. 42, no. 12, 1999, pp. 40-46.
2. Alam, Muhammad, et al. "Adaptive Authentication Mechanisms in Cybersecurity: A Review." *Journal of Information Security and Applications*, vol. 52, 2020, p. 102457.
3. Beautelement, Adam, M. Angela Sasse, and Mike Wonham. "The Compliance Budget: Managing Security Behaviour in Organisations." *Proceedings of the 2008 New Security Paradigms Workshop*, 2008, pp. 47-58.
4. Boss, S. Christian, et al. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors." *MIS Quarterly*, vol. 39, no. 4, 2015, pp. 837-864.
5. Cram, W. Alec, Dennis F. Galletta, and Paul Benjamin Lowry. "The Inconvenience-Fatigue-Workaround Path: A Longitudinal Evaluation of Cybersecurity Fatigue." *Journal of Management Information Systems*, vol. 38, no. 3, 2021, pp. 785-812.
6. Cranor, Lorrie Faith. "A Framework for Reasoning About the Human in the Loop." *Proceedings of the 1st Conference on Usability, Psychology, and Security (UPSEC)*, 2008.
7. Davis, Fred D. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology." *MIS Quarterly*, vol. 13, no. 3, 1989, pp. 319-340.
8. Florêncio, Dinei, and Cormac Herley. "A Large-Scale Study of Web Password Habits." *Proceedings of the 16th International World Wide Web Conference*, 2007, pp. 657-666.
9. Herley, Cormac. "So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users." *Proceedings of the 2009 Workshop on New Security Paradigms*, 2009, pp. 133-144.
10. Ifinedo, Princely. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory." *Computers & Security*, vol. 31, no. 1, 2012, pp. 83-95.
11. Khadka, Bijay, and Abul Bashar Sharif Ullah. "Cybersecurity Framework for Operator 5.0." *Journal of Industrial Information Integration*, vol. 42, 2025, pp. 250-264.
12. Maddux, James E., and Ronald W. Rogers. "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change." *Journal of Experimental Social Psychology*, vol. 19, no. 5, 1983, pp. 469-479.
13. Nielsen, Jakob. *Usability Engineering*. Morgan Kaufmann, 1994.
- Parsons, Kathryn, et al. "Exploring Susceptibility to Phishing in the Workplace." *International Journal of Human-Computer Studies*, vol. 120, 2018, pp. 1-13.
14. Rogers, Ronald W. "A Protection Motivation Theory of Fear Appeals and Attitude Change." *Journal of Psychology*, vol. 91, no. 1, 1975, pp. 93-114.
15. Salihu, G. A., et al. "Improved Human-Centric Cybersecurity Framework for Protecting Home Users from Social Engineering Attacks." *Direct Journal of Engineering and Information Technology*, vol. 14, no. 1, 2026, pp. 38-49.

16. Saltzer, Jerome H., and Michael D. Schroeder. "The Protection of Information in Computer Systems." *Proceedings of the IEEE*, vol. 63, no. 9, 1975, pp. 1278-1308.
17. Sasse, M. Angela, Sasha Brostoff, and Dirk Weirich. "Transforming the 'Weakest Link'—A Human/Computer Interaction Approach to Usable and Effective Security." *BT Technology Journal*, vol. 19, no. 3, 2001, pp. 122-131.
18. Stanton, Brian, et al. "Security Fatigue." *IT Professional*, vol. 18, no. 5, 2016, pp. 26-32.
19. Thaler, Richard H., and Cass R. Sunstein. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. Yale University Press, 2008.
20. Whitten, Alma, and J. D. Tygar. "Why Johnny Can't Encrypt: A Usability Case Study of PGP 5.0." *Proceedings of the 8th USENIX Security Symposium*, 1999, pp. 11-28.

