Human Factors In Cybersecurity: User/Human Behaviour Analysis.

Chetan Kharatmal
Indira College of Commerce
& Science .
Chetan.kharatmal24@iccs.ac.in

Abstract:

Human factors are vulnerability in cybersecurity because many security incidents driven by user behaviour rather than technical failures. This research paper studies human behavioural factors influencing cybersecurity outcomes, including cognitive limitations, risk assessment, usability and social challenges. The study finds common patterns like vulnerability to social engineering, securi ty fatigue, and inconsistent policy compliance by drawing on interdisciplinary li terature from cybersecurity, psychology, and human-computer interaction.the paper further studies the impact of artificial intelligence and automation on user behaviour, highlighting risks of over-depended and reduced user engagement. The paper Highlights the gap between security awareness and actual behaviour and argue for human centred, behaviour-informed security design to improve the effectiveness and sustainability of cybersecurity defences .

KEYWORDS:

Human Factors, User Behaviour Analysis, Social Engineering, Cyberpsychology, Human-Centric Security, Cognitive Biases, Artificial Intelligence, Security Awareness, Insider Threats.

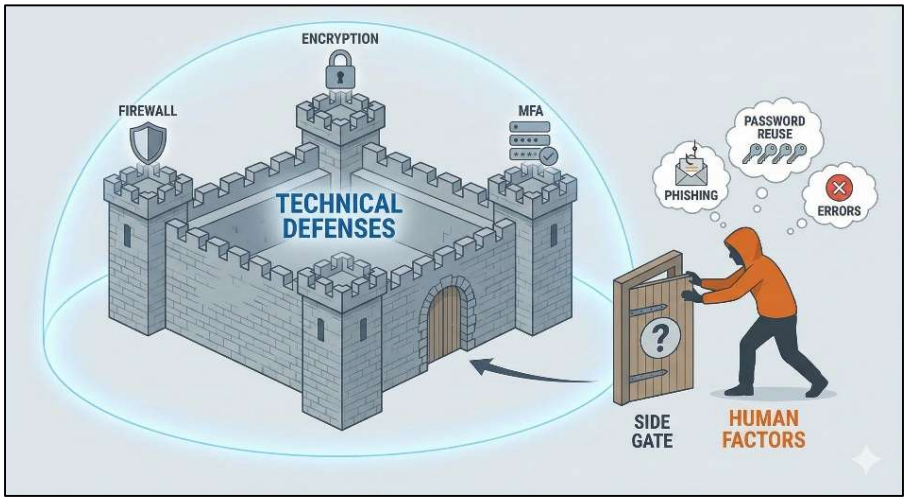
1. Introduction

The increasing use of digital technologies has made cybersecurity important for individuals, organizations, and critical infrastructure. Digital technologies have begun to support the most essential activities of the individual, including communication, finance, the delivery services, education, and working from a distance, thus producing an endless amount of data. This expanding digital footprint has risk of possible breaches and thus the need to understand the effectiveness of sustainable cybersecurity.

considerable progress has been made in the field of Cybersecurity for technical security including encryption, firewalls, intrusion detection systems(IDS), and multi-factor authentication cyber attacks continue to occur at high rates. Attacks such as malware, ransomware, phishing, financial fraud and social engineering are occurring as never before .

A growing body of research indicates that human factors play a pivot role in cybersecurity failures. Humans act as weakest part of cybersecurity for attacks through behaviours such as reuse of password, replying to phishing mails , ignoring security aspects for convenience, or overlooking security warnings. These behaviours are mostly unintentional and arise from cognitive limitations, time pressure and biased risk. Real-life studies consistently show that a large number of successful cyberattacks involves various form of human error, highlighting the importance of understanding user behaviour in security contexts.

User behaviour is influenced by various factors like psychological, social, and organizational factors. Despite security awareness efforts, a huge gap exists between users knowledge of cybersecurity and their actual real-life behaviour. Standard awareness and training programs/events often fail to change user behaviour because it does not adequately for real-world constraints, motivational factors that shape user decision-making.



Conceptual diagram of a fortress representing technical defences with a side gate.

The advance artificial intelligence (AI) and automation further complicate the human & cybersecurity relationship. AI-driven security technologies makes better threat detection and response capabilities. however, they can bring new behavioural risks, such as over-depended on automated systems and reduced user alertness .

This research studies human behavioural factors in cybersecurity through psychology, and user interaction. By integrating findings across these domains, the research observe repeated behavioural patterns including susceptibility to social engineering, security vulnerability, and outdated policy compliance and emphasizes the need for human-centred, behaviour-informed security design.

1.1 Scope and Contributions

This paper research focuses on user traits that influence cybersecurity factors, with an focus on user decision-making, behavioural vulnerabilities, and interactions between users and technology. The scope excludes deep technical study of cyber-attack and instead treats cybersecurity as socio-technical issue in which human behaviour plays important role.

The contributions of this paper are as follows:

1. **Literature Synthesis**: the research provides a review of cognitive, psychological, social, and organizational factors affecting user security behaviours, combing insights that are often addressed separately in prior work.
2. **AI and Automation Perspective:** It highlights the behavioural implications of AI based and automated security systems, identifying vulnerability such as automation bias and reduced user alertness that remain insufficiently explored.
3. **Research Gaps and Design Implications:** this research identifies key gaps in existing Technology and outlines effects of user focused, and behaviour informed security design aimed at improving the effectiveness and sustainability of cybersecurity practices.

2. **Key Human Vulnerabilities and Behavioural Patterns:**

2.1. Psychological Factors:

Cybersecurity threats increasingly exploit human psychology rather than relying solely on technical vulnerabilities. Human actions within organizations represent one of the largest security challenges, as adversaries strategically leverage psychological tendencies and behavioural inconsistencies to circumvent technological defences. Despite advance technical safeguards, insider threats whether accidental or intentional remain a critical vulnerability that organizations struggle to address

Key Psychological Vulnerabilities:

- Cognitive Biases
- Personality Differences
- Behavioural Risk Factors

2.2 Social Engineering:

Social engineering attacks exploit human psychology to deceive individuals into compromising information security, making the human element a critical vulnerability in cybersecurity systems. These attacks are fundamentally different from technical exploits because they target psychological principles and behavioural patterns. Rather than breaking through firewalls or discovering software vulnerabilities, attackers use persuasion, manipulation, and deception to convince people to reveal sensitive information or perform actions that compromise security.

The success of social engineering lies in its ability to exploit predictable human vulnerabilities. Research identifies recurring human vulnerability factors including low security awareness, emotional manipulation (such as fear and urgency), over trust in authority, and lack of behavioural control.

Cybercriminals deliberately leverage psychological weaknesses that are difficult to defend against with technology alone.

Social Engineering Cybercrimes:

- Automated Credential Stuffing
- Business Email Compromise (BEC)
- Romance and Investment Scams
- Financial Frauds

2.3 Security Awareness and Behavioural Change

2.3.1 The Theory Practice Gap

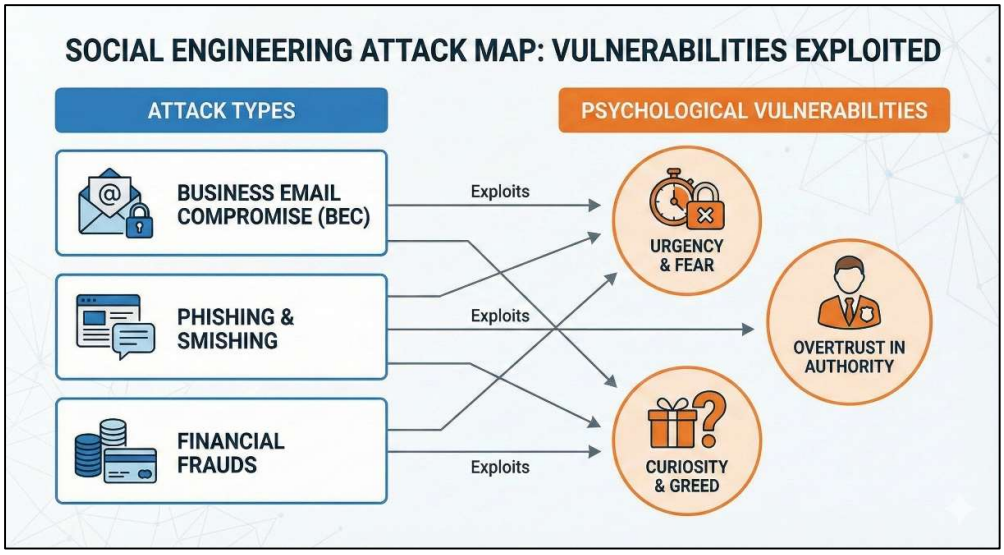
Protection Motivation Theory governs research on cybersecurity behaviour; however, mostly literature focuses on behavioural intentions rather than observed framework. Data backed research typically suggest that increased awareness does not actually translate into secure behaviour. In cases, conflicting or overly complex security rules may even worsen human vulnerabilities instead of reducing them.

2.3.2 Improving User Compliance

- Behavioural models such as the Fogg Behavioural Model offer better approach for improving cybersecurity compliance by aligning motivation, ability, and triggers. Moreover, “machine learning–based user classification techniques” enable classification of users into unique behavioural profiles, allowing organizations to Implement a personalized cybersecurity curriculum /training and targeted interventions that improve the benefits of security awareness programs.

2.4 Individual Differences and Demographics

Cybersecurity behaviour differed across each and every individuals based on demographic and experiential factors. Prior research indicates that education level, and professional background influence security knowledge and behaviour of a person. Studies on malware vulnerability have reported higher vulnerability among non-IT professionals specially one born before 1995 “Non Gen-z” and certain demographic groups, including females in specific contexts.



Infographic mapping social engineering attacks to psychological triggers

2.5 User Behaviour Analytics and Detection Methods

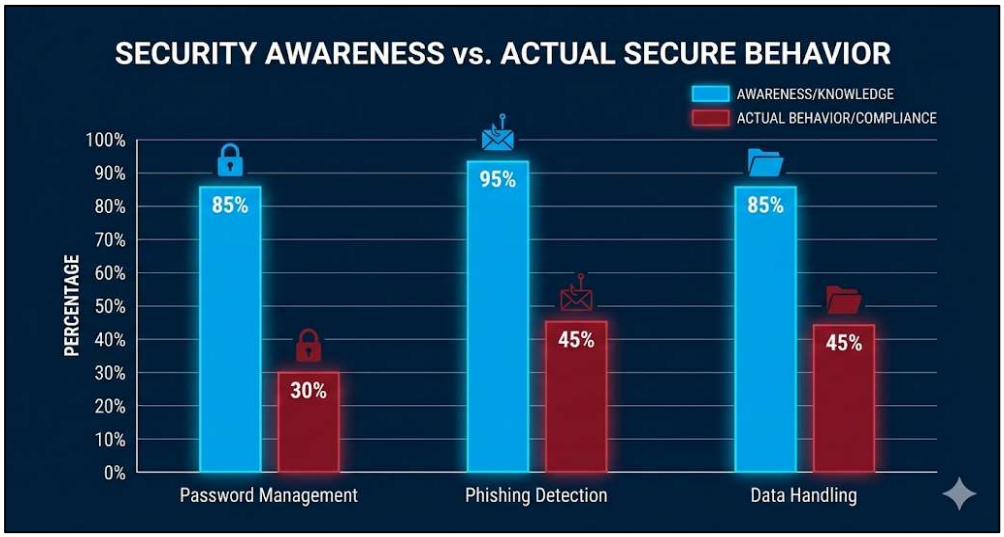
User behaviour Analytics has been an effective technique for find insider threats and breached accounts. It establishes bottom line of normal user activity and detect deviations that may indicate malicious behaviour. machine learning techniques, Research integrate with psychological and behavioural insights into cyber threat detection shows that incorporating psychometric analysis can reduce fake and enhance detection accuracy. In cloud security environments, Artificial Intelligence have been shown to outdated traditional methods in predictive threat detection, it further shows the potential of behaviour-aware security systems.

2.6 Addressing Human Error in Cybersecurity

Human error is major cause of cybersecurity incidents. Inconsistent reporting and the absence of standardized classification frameworks like ISO, limit effective mitigation. Integrating established human factors frameworks, such as the Human Factors Analysis and Classification System (HFACS) are improving incident analysis and More better cybersecurity responses.

2.7 Emerging Research Directions

Recent research priorities the need for Collaborative approaches that integrate technical security technique with a deeper understanding of human behaviour. Organizations must compile security cultures that address employee's psychological well-being, reduce anxiety through supportive measures, and transparent communication regarding security incidents. By adopting a human-cantered model alongside advance technical solutions, organizations can develop more resilient and adaptive cybersecurity defences.



Bar graph comparing security awareness vs. actual compliance

3. Positive Human Factors in Cybersecurity.

Due to raise in use of AI , The human factors have began more crucial part of cybersecurity as never before. While humans are considered as the weakest link of cybersecurity, many new research consider it as crucial defends against cyber threats. Professional has increasingly been trained for having the potential to advance technical protections and build resilient workforces that reduce organizational risk.

Key Positive Factors

3.1 Emotional Intelligence and Critical Thinking
Research shows that emotional intelligence and critical thinking are vital defences against social engineering attacks. These psychological capabilities allows to recognize and resist manipulation tactics used by attackers. Organizations that evolve these traits among their Professionals to create stronger organizational defences.

3.2 Self-Efficacy and Motivation
Studies shows that individual's confidence in their ability to protect themselves has a better positive influence on cybersecurity when employees feel capable and authorized to take security actions, they're more likely to engage in secure practices. Additionally, positive attitudes toward cybersecurity ,helps individual to tackle cyber threads.

3.3 Behavioural Compliance and Organizational Support
Top managements like Ceo, Directors and support have emerged as key enabling factors. When leadership prioritizes cybersecurity and provides necessary teams and resources, employees comply with security protocols. This makes an organizational culture where security becomes a shared responsibility rather than an imposed burden on SOC teams.

3.4Awareness and Knowledge
Cybersecurity awareness programs are highly effective when they address emotional, cognitive, and behavioural components. Employees who have knowledge about cybersecurity threats and maintain positive approach toward security measures data shows significantly better protective behaviours.

4 Human-Centric Security Approaches

4.1 Collaboration Between Humans and AI

Research shows that the integration of human with artificial intelligence creates better security Envirnment. Humans are great at providing contextual understanding, ethical judgment, and adaptive reasoning, while Artificial Intelligence is responsible speed and pattern recognition. This partnership forms the foundation for Best security operations.

4.2 Psychological Resilience and Training

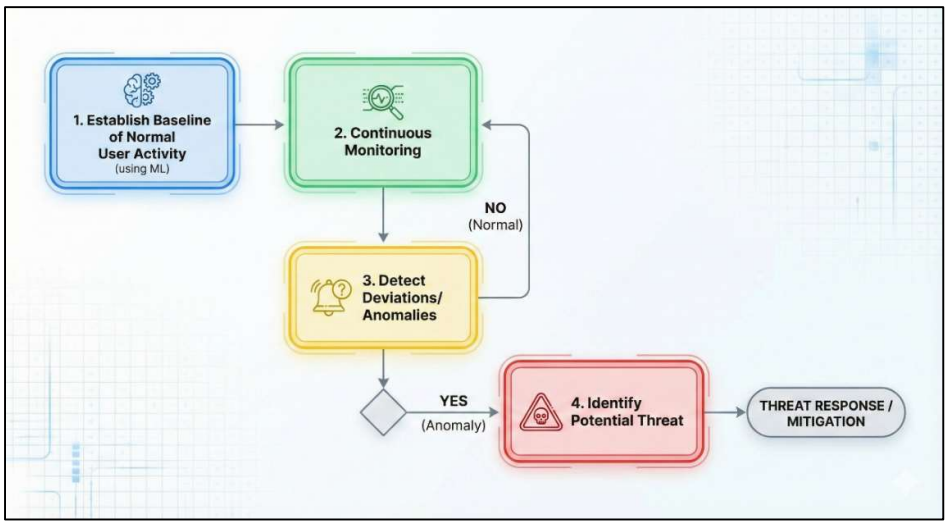
Effective cybersecurity technique should incorporate personalized training programs and emotional intelligence development. A human-centric cybersecurity training framework that includes gamified learning and decision-support systems reduces vulnerabilities and promotes Cybersecurity compliance.

4.3 Organizational Culture Development

Creating and maintaining a positive cybersecurity culture in at levels strengthens defences. This involves providing an environment where employees understand security not as punishment-driven compliance, but as a responsibility for organizational protection.

4.4 Practical Benefits

This research indicates that when organizations aims positive human factors effectively, they experience improves in cybersecurity posture. An integrated approach that addresses user's cognitive characteristics, organizational culture, and technological innovations leads to more effective Cybersecuritythan technology-alone solutions.



User behaviour Analytics (UBA) flow diagram

CONCLUSION :

This paper has analysed the role of human Prox related to cybersecurity. The study has demonstrated how many incidents of cybersecurity failure can result from human behaviour rather than just from technology itself. Looking through the range of literature from different fields of study has helped the author of the paper arrive at some of the key human vulnerabilities such as cognitive biases. Another important finding has been the role of users not being just a weakest link within a system but being able to positively help towards a more secured system. The study has helped refine how human behaviour can result in vulnerabilities such as over-reliance on artificial intelligence. This study encourages balancing human behaviour with artificial intelligence. In conclusion, this study has helped emphasize that a systematic approach to understanding both the human behaviour element as well as a techno-methodology for a solution for securing a system would need to be combined for any successful results. Future studies would need to help promote a human-centric model of study.

Illustration of interlocking gears representing human expertise and artificial intelligence

References :

1. M. O. Ijiga, H. S. Olarinoye, F. A. B. Yeboah, and J. N. Okolo, “Integrating Behavioral Science and Cyber Threat Intelligence (CTI) to Counter Advanced Persistent Threats (APTs) and Reduce Human-Enabled Security Breaches,” Mar. 2025.
2. M. S. Tsauri, “Human Vulnerabilities to Social Engineering Attacks: A Systematic Literature Review for Building a Human Firewall,” Aug. 2025.
3. J. Jeong, J. Mihelcic, G. Oliver, and C. Rudolph, “Towards an Improved Understanding of Human Factors in Cybersecurity,” International Conference on Communications in Computing, Dec. 2019.
4. N. Sugunaraj, “Human Factors in the LastPass Breach,” arXiv.org, May 2024.
5. X. Liu, “The Cyber Acumen,” Analyzing Human Behavior in Cyberspace, 2019.
6. M. E. Edwards, T. Morris, J. Chen, and J. D. Still, “SMiShing Attack Vector: Surveying End-User Behaviour, Experience, and Knowledge,” Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Sep. 2023.
7. Google Gemini generated image, "Bar graph comparing security awareness vs. actual compliance," [AI-generated image], Dec 2025.
8. Google Gemini generated image, "Bar graph comparing security awareness vs. actual compliance," [AI-generated image], Dec 2025.
9. Google Gemini generated image, "User Behavior Analytics (UBA) flow diagram," [AI-generated image], Dec 2025.
10. Google Gemini generated image, "Illustration of interlocking gears representing human expertise and artificial intelligence," [AI-generated image], Dec 2025.