**Editor’s Comment:**

The manuscript explores an increasingly critical and timely issue in cybersecurity—the role of the human factor—through a multidimensional lens that integrates psychological, organizational, and technical insights. The authors offer a conceptually rich discussion that highlights the paradoxical role of human behavior as both a cornerstone of cybersecurity and a principal vulnerability. Key strengths of the manuscript include its interdisciplinary synthesis, drawing from psychology, organizational behavior, and cognitive science. Particularly notable are the discussions on decision-making biases, emotional intelligence, and security fatigue, as well as the nuanced exploration of social engineering strategies like pretexting and phishing. The outlined future research directions, touching on areas such as neurocognitive studies and behavioral economics, are insightful and valuable for advancing the field. However, moderate revisions are required before the manuscript is suitable for publication. Methodological clarity needs improvement, particularly in detailing how literature sources were selected and synthesized. While statistical summaries are referenced, the lack of original empirical findings somewhat limits the contribution. Structurally, the integration of figures and tables could be improved for better coherence with the narrative. Additionally, deeper critical engagement with existing empirical studies and clearer identification of the manuscript's original contributions would enhance its scholarly impact.

**Editor’s Details:**

Dr. A. Suresh, SRM Institute of Science & Technology, India