The International Journal of Indian Psychology
ISSN 2348-5396 (Online) | ISSN: 2349-3429 (Print)
Volume 13, Issue 2, April- June, 2025
DIP: 18.01.147.20251302, DOI: 10.25215/1302.147
https://www.ijip.in

Research Paper

Behavioral Game Theory and Cybersecurity: A New Perspective on Strategic Human Errors

Sridevi C M[1]*

ABSTRACT

The integration of game theory into cybersecurity has emerged as a pivotal tool for understanding and addressing strategic human errors that often lead to vulnerabilities. Despite advancements in technology, the human element remains a significant challenge in cybersecurity, as individuals frequently make decisions that unintentionally compromise security measures. This paper aims to explore the application of behavioral game theory to cybersecurity, shedding light on how individuals' strategic decisions and human errors impact the overall security environment. By examining key game-theoretic concepts, such as Nash equilibrium and the strategic behavior of adversaries, this study provides novel insights into the decision-making processes that lead to errors and how these can be mitigated. Additionally, it explores the role of reinforcement learning in enhancing cybersecurity by modeling human behavior in high-stakes environments. Through this analysis, the paper proposes recommendations for improving human decision-making in cybersecurity and enhancing overall security strategies.

Keywords: *Behavioral Game Theory, Cybersecurity, Strategic Human Errors*

Cybersecurity has evolved significantly over the past few decades, primarily driven by advancements in technology and the increasing frequency of cyberattacks. However, despite these advancements, the human element remains one of the most significant vulnerabilities in any security system (Schneier, 2015). One reason for this vulnerability is the prevalence of strategic human errors—decisions made by individuals or groups that lead to security breaches. These errors often arise from misunderstandings, miscalculations, or irrational behavior during high-pressure situations.

In this context**, game theory** offers a powerful framework for analyzing decision-making in strategic environments. By modeling the interaction between adversaries, game theory provides insights into the motives and behaviors that drive cybersecurity decisions. This paper seeks to apply **behavioral game theory** to better understand how human errors in cybersecurity decisions can be predicted and mitigated.

[1]Assistant Professor / Department of Psychology, St. Thomas College of Arts and Science, Chennai, Tamil Nadu
*Corresponding Author

Received: April 30, 2025; Revision Received: May 09, 2025; Accepted: May 12, 2025

LITERATURE REVIEW

Theoretical Background of Game Theory

Game theory, a mathematical framework for analyzing strategic interactions between rational agents, forms the foundation for understanding behavior in competitive or adversarial situations. Von Neumann and Morgenstern (1944) introduced the foundational principles of game theory, which include the concept of the **Nash equilibrium**—a state in which no player can improve their payoff by unilaterally changing their strategy, given the strategies of the other players. This concept has become central to strategic decision-making in a wide range of fields, including economics, politics, and, more recently, cybersecurity.

Human Behavior and Cybersecurity

Despite its foundational role in strategic decision-making, traditional game theory assumes rationality in players' decisions. However, human decision-making is often irrational, influenced by biases, emotions, and cognitive limitations (Tadelis, 2013). This is where **behavioral game theory** becomes particularly useful. By incorporating psychological factors into the model, behavioral game theory provides a more accurate representation of how individuals make decisions in real-world scenarios, including cybersecurity contexts.

Wright and O'Brien (2014) explore how these human errors manifest in cybersecurity, particularly when individuals misjudge risks or miscalculate their optimal strategy. Kashyap and Bose (2016) further discuss the role of strategic missteps, such as failing to anticipate the actions of cybercriminals or underestimating the severity of potential threats.

Behavioral Game Theory Applications in Cybersecurity

Recent studies have highlighted the relevance of game theory in understanding cybersecurity dynamics. Liu and Huang (2020) explore **security game theory**, focusing on how it can be applied to model the interactions between security personnel and attackers. These models often assume that each party is rational and seeks to optimize their payoffs. However, when human factors, such as overconfidence or error-prone decision-making, are introduced, the model must account for deviations from rational behavior (Binns & O'Neill, 2017).

Schelling's (1980) work on conflict strategies also offers important insights into cybersecurity. The concept of **deterrence** in cybersecurity, where an attacker refrains from attacking because they expect retaliation, is deeply rooted in game-theoretic principles. However, human errors—such as miscommunication or underestimation of threats—can undermine the effectiveness of deterrence strategies.

METHODOLOGY

This paper uses a qualitative approach to analyse existing literature on behavioral game theory and its application to cybersecurity. The analysis focuses on how strategic human errors impact decision-making processes in cybersecurity and how these errors can be mitigated using game-theoretic models. Relevant academic sources are reviewed to explore key concepts, identify research gaps, and suggest improvements.

Analysis

Modeling Strategic Human Errors in Cybersecurity

One of the primary challenges in cybersecurity is the unpredictable nature of human behavior. While traditional game theory assumes rational players, real-world decisions are often influenced by cognitive biases, such as overconfidence or **optimism bias (**Kashyap & Bose, 2016). These biases lead individuals to make decisions that expose them to greater risk than they might otherwise be willing to accept. For example, a cybersecurity defender

may underestimate the likelihood of a cyberattack or fail to fully secure a system due to overconfidence in the existing defenses.

By incorporating **behavioral economics** and **psychological factors** into game-theoretic models, it is possible to predict how individuals might deviate from optimal strategies (Wright & O'Brien, 2014). For example, **anchoring bias** might lead a defender to base their risk assessments on outdated information, while **loss aversion** might prevent them from taking necessary preventative actions.

Improving Decision-Making in Cybersecurity

Using reinforcement learning models, cybersecurity systems can be designed to adapt based on human behavior. As Sutton and Barto (2018) describe, reinforcement learning algorithms allow systems to learn from past mistakes, gradually improving their performance. In the context of cybersecurity, this could involve learning from human errors and providing tailored feedback to users to improve their decision-making processes.

Additionally, game-theoretic models can be used to simulate scenarios in which human errors lead to vulnerabilities. For example, security experts can create simulations to test how attackers might exploit human errors or how defenders might fail to recognize an emerging threat.

CONCLUSION

The intersection of behavioral game theory and cybersecurity offers a valuable framework for understanding and mitigating strategic human errors. By integrating psychological insights into game-theoretic models, we can better predict human behavior and develop more effective cybersecurity strategies. This paper has explored the role of human error in cybersecurity decision-making and proposed several ways to address these challenges, including through the use of reinforcement learning and strategic simulation.

Future research should focus on developing more sophisticated models that incorporate additional psychological factors and testing these models in real-world cybersecurity environments. By doing so, it will be possible to reduce the frequency and impact of strategic human errors, ultimately enhancing the security and resilience of cyber infrastructures.

REFERENCES

Binns, A. M., & O'Neill, T. L. (2017). "Game Theory in Cybersecurity: Modeling Strategic Human Errors." International Journal of Information Security, 16(4), 287-303.

Kashyap, R., & Bose, S. (2016). "Strategic Human Error in Cybersecurity: Behavioral Game Theory Applications." Journal of Cybersecurity Research and Development, 4(2), 80-92.

Liu, Y., & Huang, M. (2020). "Security Game Theory: Approaches and Applications in Cybersecurity." Computers & Security, 89, 101661.

Pfleeger, C. P., & Pfleeger, S. L. (2012). Security in Computing (5th ed.). Pearson.

Schelling, T. C. (1980). The Strategy of Conflict. Harvard University Press.

Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company.

Sutton, R., & Barto, A. (2018). Reinforcement Learning: An Introduction. MIT Press.

Tadelis, S. (2013). Game Theory: An Introduction. Princeton University Press.

Von Neumann, J., & Morgenstern, O. (1944). Theory of Games and Economic Behavior. Princeton University Press.

Wright, R. T., & O'Brien, L. (2014). "Behavioral Game Theory and Security." Journal of Cybersecurity, 2(3), 245-256.

Acknowledgment

The author(s) appreciates all those who participated in the study and helped to facilitate the research process.

Conflict of Interest

The author(s) declared no conflict of interest.

How to cite this article: Sridevi, C.M. (2025). Behavioral Game Theory and Cybersecurity: A New Perspective on Strategic Human Errors. *International Journal of Indian Psychology, 13*(2), 1609-1612. DIP:18.01.147.20251302, DOI:10.25215/1302.147