The current issue and full text archive of this journal is available on Emerald Insight at:
https://www.emerald.com/insight/0959-3845.htm

Understanding the process of building institutional trust among digital payment users through national cybersecurity commitment trustworthiness cues: a critical realist perspective

Received 9 May 2023
Revised 29 September 2023
Accepted 18 October 2023

Ben Krishna, Satish Krishnan and M.P. Sebastian
Information Systems Area, Indian Institute of Management Kozhikode, Kozhikode, India

Abstract

Purpose – The current body of empirical research regarding the impact of trust in the cybersecurity commitment of institutions on digital payment usage has focused solely on a macro-level analysis, overlooking the intricate dynamics between institutions' cybersecurity commitments and the trust levels of digital payment users. In light of this limitation, this study aims to offer a more comprehensive understanding of this complex relationship.

Design/methodology/approach – A case study was conducted on digital payment users in India through the critical realist lens. To gather data, interviews and focus group discussions were conducted with digital payment users from various regions of the country.

Findings – The citizen-centric outcomes of the national cybersecurity commitment (performance and responsiveness) are the most prominent and impactful trust indicators. These outcomes play a crucial role in shaping digital payment users' perception and trust in the cybersecurity commitment of public institutions. Individuals' value positions also influence trust judgments, as it is essential to recognize the value tensions that may arise due to security implementation and their congruence with citizens' values.

Research limitations/implications – The findings of this study have significant implications for policymakers. They are potentially an artifact of the security and perception of digital payment users and the cultural uniqueness of digital payment users in India.

Originality/value – The study proposes a holistic understanding of the relationship between institutions' cybersecurity commitments and the trust levels of digital payment users. It offers a qualitative evaluation of how digital payment users perceive and construe efficient information security management implemented by public institutions.

Keywords Cybersecurity commitment, Institutional trust, Digital payment, Critical realism, India

Paper type Research paper

Introduction

Digital payment users exhibit a heightened awareness of the numerous security threats (e.g. unauthorized access to customer data, identity theft, cybersecurity attacks, customer errors and systems vulnerabilities) prevalent within the digital financial landscape, resulting in widespread distrust towards various financial platforms and services (Lee *et al.*, 2018, 2020; Ru and Schoar, 2016). Further, the digital payment landscape is evolving, with various payment aggregators, digital financial platforms, and traditional financial services creating new linkages and dependencies in the financial ecosystem. Thus, consumers' perceived risks associated with novel digital financial technologies significantly influence the acceptance and

Satish Krishnan thanks the Indian Institute of Management Kozhikode's Chair Associate Professorship for supporting this research.

Information Technology & People
© Emerald Publishing Limited
0959-3845
DOI 10.1108/ITP-05-2023-0434