12-15-2024

A Data-Driven Analysis of Indian startup Reaction to Cybersecurity Incidents

Anu Rao
Indian Institute of Technology Jodhpur, anrao2014@gmail.com

TREO
Technology, Research, Education, Opinion

A Data-Driven Analysis of Indian startup Reaction to Cybersecurity Incidents
Data breaches and Indian startups

Anu Rao(anrao2014@gmail.com), Amit Singh(amtkds@gmail.com), Devi Prasad Dash(dpdash@iitj.ac.in)

Technology startups also known as tech startups, are experiencing rapid growth within the global entrepreneurial ecosystem. Over the last five years, India has six established startup hubs with 51% Compound Annual Growth Rate (CAGR), four emerging startup hubs with 55% CAGR, and four nascent startup hubs with 45% CAGR (NASSCOM 2019). There are startups which aim to deliver scalable, simplified, and consistent customer experience, but lack the financial means, expertise, and tools to adequately protect themselves. They emphasis on growth over security, reliance on third-party services, and lack of comprehensive policies, making attractive targets for malicious actors' which focusses on exploiting the weaknesses in the digital infrastructure. These types of startups fall under the category of constrained resource startups. Almost half of all cyberattacks affect such startups leading to significant losses including system quality, service quality, and system quality (Chung 2020). To restore the relationships with stakeholders after experiencing data breaches, startups employ a range of recovery and response strategies. However, the impact of these response strategies on stakeholders' behavior following such incidents remains uncertain.

Based on the integration of Resource-Based View (RBV) and Institutional Theory (IT) (DiMaggio and Powell, 1983), we aim to understand both internal resource constraints and external institutional pressures that influence how constrained resource startups approach and manage cybersecurity under data breach environment. Through a multimethod study, we aim to identify the response strategies adopted by constrained-startups through content analysis from established reports in study 1, highlighting different combinations of security controls following data breaches. Our study particularly focusses on fintech, and health tech Indian startups as they are the most targeted industries (Verizon, 2024). In study 2, we would try to examine how these response strategies influences startup's performance (including system quality, service quality and information quality) and investors affected by data breaches. In study 3, we examine the investor's behaviour to constrained-startup's responses in maintaining their reputation damage due to data breach. I would explore this through an event study. We would aim to contribute to cybersecurity and threat management research by outlining various responses strategies particularly adopted by constrained resource startups following the data breach incidents.

References

Chung, M. (2020). Signs your cyber security is doomed to fail. *Computer Fraud and Security,* 2020(3), 10-13. https://doi.org/10.1016/S1361-3723(20)30029-4

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, *48*(2), 147–160. https://doi.org/10.1515/9780691229270-005

NASSCOM. (2019). Indian Tech Start-up Ecosystem.

Verizon. (2024). Data Breach Investigations Report. Verizon Communications Inc. https://www.verizon.com/business/resources/reports/dbir/