Vindhyan Bloom

ISSN-2319-8478
Vol-15 Issue-4, July 2026

A Referred Peer Review Research Journal

Vindhyan Bloom

ISSN-2319-8478 Vol-15 Issue-4, July 2026

Manuscript Information	*Reviewed* 10-07-2026	*Accepted* 16-07-2026	*Published* 31-07-2026	*Paper No.* VB-2026-07-04
DOI	*https://doi.org/10.5281/zenodo.21880733*			

Behavioural Finance as A Resilient Strategy for Indian Banking Cybersecurity

M.Vignesh, *Assistant Professor, Department of Management Studies, The American College,* ***Madurai, Tamilnadu, India***

"*Cybersecurity isn't about avoiding risk — it's about managing it intelligently*." — **Adam Fletcher**, CISO, Blackstone

Abstract

Prevention is better than cure is a known adage. But customers failed to keep abreast with the alert messages, especially in the banking sectors. Even they aware of the prevalent cybercrimes as phishing, vishing etc., ultimately they are the victims. The concept of https , cryptography are obsolete. Now-a-days, novel cyber securities are required to combat the newly emerging cyber threats. The concept of behavioural finance plays a major role in preventing the cybercrimes in banks by addressing the human factor as their behaviour, which is considered to be the weakest link in cybersecurity. Behavioural finance includes altering the consumer behaviour by psychological means and also by the architecture. The Zero Trust Architecture (ZTA) is the much sought after protocol for the banks. It is based on the security concept of "Never Trust, always verify". The system is aimed to prevent the security lapses in the traditional system. In other words, it aims at utilizing the concept of behavioural finance with analytics in fraud detection. With the increase in ICT and IoT devices, ZTA ensures the security between the bank and the individual customer or in B2B transactions. It acts as a resilient solution to the bankers and the customers. This paper discusses with some of the resilient strategies of banking cybersecurity which includes the behavioural finance and ZTA.

Keywords: behavioural finance, zero trust architecture (ZTA),biases, cybercrime, nudge, loss aversion.

Introduction

Cybercrimes are in the alarming rate with the technology development . It was skyrocketed upto 36 lakh fraud activities with a whooping loss of Rs. 22,845 crore in 2024 (The Times of India). The irony is RBI's website faces 61 million cyberattacks in the Q3 of FY26 (Outlook Money). Private sector banks are most affected than the public sector banks. Kotak Mahindra Bank, Axis Bank, State Bank of India, HDFC Bank, and ICICI Bank are in the top five ranks of highest amount lost in cybercrime. Out of the Indian states, Maharashtra accounts for more than one-fourth of the amount lost due to cyberfraud. (Zakariasiddiqui,sabirahamed, 2024).

Behavioural finance can be used as a resilient tool to combat the cybercrime amongst the banks. It focuses on the human behaviour on their banking which

ISSN-2319-8478
Vol-15 Issue-4, July 2026

includes their emotions, decision-making patterns which impact on their financial actions. It has been observed that most of cybercrimes related to the banks as phishing, OTP fraud are not due to the technological backdrop, but because of the biased human behaviour.

Resilient strategies in banking includes how the banks adopt , survive and recover from the threats in form of cyberattacks. In the simplest term, an alert message as " This transaction may result in financial loss " may change the behaviour of the individual to think and act accordingly.

The resilient measures include inclusion of state-of-the-art tools as zero trust architecture (ZTA), which is discussed here.

Review of Literature

Cyberattacks will have a negative impact on India's financial ecosystem (Bora, 2025). Behavioural aspects of the customers enable to mitigate the effects of cyberattacks (Huang et al.,2011). Individuals often emphasize cybersecurity risks as a means to anticipate potential threats, fostering a sense of security imagination and fictional fear (Bruijn and Janssen 2017).Cyber-resilience will be defined as the capacity to withstand and to get recovered from the aftermath shocks caused by cyber risks. (BenoıˆtDupont, 2019). Financial institutions spent more towards the firewall systems, intrusion detection and prevention systems (IDPS) in order to protect the valuable data.(Dr. Amey Rajiv Naik , Dr. Trilok Singh , 2024). Cybersecurity is considered to be essential and it should not be ignored. (Ambore et al., 2017) . Rugina (2023) highlighted the importance of international collaboration in innovation and research in combating the cybercrimes. A collaborative system of proactive threat intelligence, continuous monitoring, and incident response planning into the cybersecurity framework of banks are essential for the early detection of cyber threats . (Dawodu et al. 2023). The common cybercrimes in online banking are phishing attacks, malware and man-in-the-middle (MITM) attacks, which exploit the communication between a user and the banking server. (Khrais 2015).

BEHAVIOURAL FINANCE STRATEGIES

1. **Preventing frauds through Loss aversion**:According to the Loss aversion concept mentioned by Kahneman and Tversky'sin Prospect Theory (1979) , the pain of losing is more intense than the pleasure of gaining an equivalent amount. Customers should be given awareness by the prompting the messages as , " your transaction may lose Rs.10,000/ if it is fraudulent", "this transaction might be risk". This is to revert the hasty decisions .
2. **Nudging secure behaviour :**Nudges are the smaller , low-cost changes done in a system which alters the behaviour of the customers. Nudging secure behaviour includes designing the digital system as nudges to modify the behaviour of the customer. This can be done by asking questions as, " Do you trust this recipient ?" and using colour cues and red flags for suspicious transactions. Utilisation of "Pause and think " nudges before every transactions can be implemented.
3. **Overcoming herd mentality among the customers :** This includes educating the users and to prevent them from herd mentality to get rid off from cryptoscams, fake investment apps .
4. **Personalised risk communication:**As different customers respond differently to risk by the way in ignoring

ISSN-2319-8478
Vol-15 Issue-4, July 2026

messages as an optimism bias, trusting known-looking emails or messages as a familiarity bias, a personalized warning message must be communicated in view of sudden large transfers, logins from unusual locations, changes in habitual transactions.

Zero Trust Architecture (Zta)

The logic of zero trust architecture envisages " Never trust, always verify" to attain a resilient goal to "prevent , absorb, recover and adopt to disruptions "

The Zero Trust Architecture (ZTA) is made up of several layers of protocol as ,

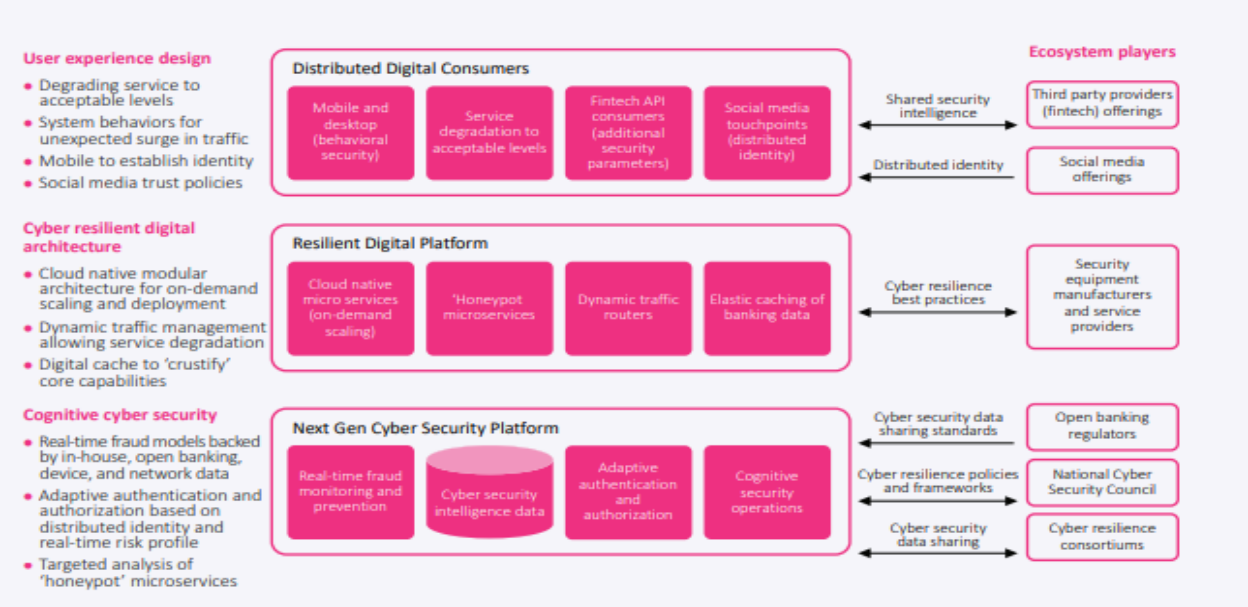
Layer 1: which enforces the concept of "nevertrust , always verify" , so that every customer's gadget or console must be equipped with multi-factor authentication (MFA) with biometrics, and microsegmentation in the ZTA divides networks into small , isolated zones which prevents the lateral movement of the information. This is a proactive system to prevent cybercrime.

Layer 2: comprises of the behavioural finance AI engine which enables the banking system resilient. It continuously checks for the cognitive bias exploitation as fraud alerts, messages and fake informations and as a watchdog for transaction anomalies.

Layer 3: The zero trust decision support system which prompts for the decision to be taken by the banking system. The SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) system prompts the function to be done or halted.

Layer 4: The resilience and the firewall system closes the fake operation.

Figure 1: Future ready cyber resilience model for next-gen digital banking by TCS



Source: www.tcs.com

Conclusion

The resilient measures in cybersecurity must be aimed to reduce the over confidence, biased approach, herd mentality. A well-structuredunifedUser and Entity Behavior Analytics (UEBA) policy framework must be implemented. At the macro level, Digital Personal Data Protection Act, 2023must be strictly

ISSN-2319-8478
Vol-15 Issue-4, July 2026

deployed among the banks. Just as the European Union's Digital operational Resilience Act (DORA) must be enacted to ensure a safer banking. At last, the behavioural finance should be viewed as a strategic pillar to enhance the cybersecurity . It must be developed as a more secure, inclusive financial ecosystem that can withstand any type of cyber threats. The scalability of such systems depends only when it eliminates the threatsthat exploit human vulnerabilities as biases, heuristics, overconfidence, and lack of awareness.

References

- Ambore, S., Richardson, C., Dogan, H., Apeh, E. and Osselton, D., 2017. A resilient cybersecurity framework for Mobile Financial Services (MFS). Journal of Cyber Security Technology, 1(3-4), pp.202-224.
- Amey Rajiv Naik , Trilok Singh Safeguarding India's Financial Infrastructure: Strategies and Techniques for Cybersecurity Risk Mitigation International Journal of Engineering Applied Science and Management ISSN (Online): 2582-6948 Vol. 5 Issue 10, October 2024
- BenoıˆtDupont, The cyber-resilience of financial institutions: significance and applicability Journal of Cybersecurity, 2019, 1–17
- Bora, Aman and Rawat, DeepaMehra, Cyber Resilience in Bharat: Safeguarding the Pillars of Indian Democracy and National Security (April 01, 2025).
- de Bruijn, H., and M. Janssen. 2017. Building cybersecurity awareness: the need for evidence-based framing strategies. *Government Information Quarterly* 34 (1): 1–7
- Dawodu, S.O., Omotosho, A., Akindote, O.J., Adegbite, A.O. and Ewuga, S.K., (2023). Cybersecurity risk assessment in banking: methodologies and best practices. Computer Science & IT Research Journal, 4(3), pp.220-243.
- Huang, D.-L., P.-L. Patrick Rau, G. Salvendy, F. Gao, and J. Zhou. 2011. Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies* 69 (12): 870–883.
- Kahneman, D., &Tversky, A. (1979). Prospect theory. An analysis of decision making under risk,*Econometrica*, 47 (2), 263-292
- Khrais, L.T., (2015). Highlighting the vulnerabilities of online banking system. Journal of Internet Banking and Commerce, 20(3), pp.1-10.
- Rugina, J.M., (2023). Through The Eyes Of Attackers: A Comprehensive Analysis Of Cybersecurity Strategies In International Relations. Afro Eurasian Studies, 12(1), pp.40-57.
- Zakariasiddiqui,sabirahamed**,** Cyber fraud in banking transactions surges in FY24, 2024

Webliography

- https://www.geeksforgeeks.org/ethical-hacking/zero-trust-architecture-in-security/
- https://hal.science/hal-04686453v1/document
- https://www.tcs.com/content/dam/global-tcs/en/pdfs/insights/whitepapers/cyber-resilience-next-gen-digital-banking.pdf