UNIVERSITI TEKNOLOGI MARA

DEVELOPING A CYBERSECURITY CULTURE MODEL AMONG ONLINE BANKING USERS IN NIGERIA

JAMILU GARBA

Thesis submitted in partial fulfilment
of the requirement for the degree of
Doctor of Philosophy
(Information Technology)

Faculty of Computer and Mathematical Sciences

October 2025

ABSTRACT

This research examines the interplay of human factors influencing cybersecurity culture among online banking users in Nigeria and develops a tailored model to address the vulnerabilities inherent in user behavior. The increasing reliance on online banking in Nigeria has amplified the need for robust cybersecurity measures to mitigate the growing threat of cyberattacks. While technological solutions are essential, human factors play a critical role in shaping cybersecurity culture, particularly in developing economies with unique socio-economic challenges. Grounded in the Theory of Planned Behavior (TPB), this study identifies critical constructs such as cybersecurity awareness, education, policy compliance, interpersonal trust, and social norms as determinants of a secure cybersecurity culture. Employing a mixed-methods approach, the qualitative phase involved in-depth interviews with cybersecurity experts to validate the cybersecurity culture model, ensuring its relevance to Nigeria's unique context. The quantitative phase surveyed 392 online banking users, employing Partial Least Squares Structural Equation Modeling (PLS-SEM) to evaluate the relationships among the identified factors. The findings reveal significant associations between cybersecurity culture and constructs such as awareness, education, and policy compliance, while interpersonal trust exhibited no significant influence. This study provides actionable insights for financial institutions, policymakers, and cybersecurity professionals, offering a robust framework to enhance user-centric cybersecurity strategies. The proposed model serves as a practical tool for addressing behavioral vulnerabilities and fostering a proactive cybersecurity culture, ensuring the resilience of Nigeria's online banking sector against ever-evolving threats.

Keywords: Cybersecurity Culture, Human Factors, Online Banking, Theory of Planned Behaviour, Cybersecurity Culture Model

ACKNOWLEDGEMENTS

Alhamdulillah, all praises, and adoration are due to Almighty Allah who has spared my life and enabled me to complete my PhD work. Peace and Allah's blessing be unto his chosen servant, his family, companions, and those who follow his path till the day of Judgement.

I would like to extend my sincere thanks to my supervisor, Dr. Jasber Kaur and co-supervisor Dr. Emma Nuraihan Mior Ibrahim for their support during my research. Their guidance, support, and suggestion always motivate me move forward. Their recommendation has always been helpful. Being able to provide their time during the research was very much appreciated. It has been a great pleasure to have them as my supervisors. I appreciate all of their patience and efforts.

My family serves as the foundation of my inspiration. My sincere and deepest thanks to my father, Alh Garba Na'aja, and my mother, , for their constant players, love, support, and sacrifice.

I extend my heartfelt thanks to my dear brother, sisters, and friends for their constant prayers. Their words of encouragement and support have been a constant source of motivation and inspiration throughout my doctoral journey.

Finally, I would like to acknowledge the support of all those who have played a part, no matter how small, in my research. Your contributions have not gone unnoticed and are deeply appreciated.

TABLE OF CONTENT

CHAPTER 1
INTRODUCTION

1.1 Background

In recent years, Nigeria's financial landscape has undergone changes due to the widespread adoption of online banking services. These services provide easy access, and ease of use, reducing the reliance on extensive physical locations for storing papers, files, and documents within the banking sectors. This digital development brings new cybersecurity challenges to online banking users. For ensuring the survival of banking sectors, especially online banking users in a highly secure cyberspace while interacting with online services, it is essential to protect both information assets and customers from cyberthreats. Chowdhury, Adam, and Teubner (2020); Singh, Gupta, and Ojha (2019); & Brickley, Thakur, & Kamruzzaman (2021) have classified cybersecurity solution into technical and non-technical solutions. Technical solution deal with aspect such as firewall, intrusion detection systems (IDS), intrusion prevention system (IPS), and many more, while non-technical solution focus on human actions. Additionally, Mark, Iryna, and Helge (2019); & Wong et al. (2019) have emphasized that cybersecurity is not solely a technical concern but also involves human actions. Most of the banking sectors already have the technical solutions to cyberthreats in place. But mitigating or minimizing cybersecurity vulnerabilities also requires a focus on enhancing the cybersecurity culture among users. This cultural enhancement can positively influence users' behaviour and contribute to a more secure online environment.

The foundational step of this research is based on examining the literature review on cybersecurity, cybersecurity culture, human factors, and online banking. Various literature emphasized the impact of human action in cybersecurity vulnerabilities. Zwilling et al. (2020); Zimmermann and Renaud (2019); & Gratian et al. (2018) recognized human as the weakest links in cybersecurity. This shows that there is need for understanding the human factors influencing cybersecurity culture. Among the major benefits of a cybersecurity culture is the protection of information assets and also the users from cyberthreats. This protection, in turn directly mitigates threats posed by user behaviour to information assets (Veiga et al., 2020). Therefore, enhancing cybersecurity culture is essential for online banking users, as it can positively impact