International Journal of Cyber Behavior, Psychology and Learning
Volume 15 • Issue 1 • January-December 2025

Emerging Technologies as a Mediating Factor Between Causes of Cyberfraud and Cyberfraud Perpetration in the South African Banking Industry

Oluwatoyin Esther Akinbowale
https://orcid.org/0000-0001-5886-3018
Faculty of Economics & Finance, Tshwane University of Technology, Pretoria, South Africa

Heinz Eckart Klingelhöfer
https://orcid.org/0000-0001-8715-0519
Faculty of Economics & Finance, Tshwane University of Technology, Pretoria, South Africa

Mulatu Fekadu Zerihun
https://orcid.org/0000-0003-4797-928X
Faculty of Economics & Finance, Tshwane University of Technology, Pretoria, South Africa

Polly Mashigo
Faculty of Economics & Finance, Tshwane University of Technology, Pretoria, South Africa

ABSTRACT

The purpose of this study is to investigate the relationship between the factors responsible for cyberfraud perpetration and the rate of cyberfraud perpetration in the South African banking industry using technology as a mediating variable. Structured questionnaire was employed as survey instrument. Using purposive sampling, it was distributed to 42 selected staff members of the 17 licensed banks in South Africa. The use of emerging technologies was found to have positive and significant relationship with internal controls, accountability, record keeping and ethical culture. This is justified by their p-values less than 0.05 except for the relationship between technology and poor organisation whose p-value was greater than 0.05. Overall, the mediating variable (technology) was found to indeed influence the rate of cyberfraud perpetration in the South African banking industry. This study provides an insight into the factors responsible for cyberfraud perpetration in South Africa and the moderating role of technology to reduce cyberfraud perpetration.

KEYWORDS

Cyberfraud, Banking Industry, Mediation Analysis, Technology

INTRODUCTION

The United Nations (UN) report "Cybersecurity and New Technologies" (2023a) indicated that there is increasing concern over threat actors' misuse of information communication technologies (ICT), particularly the Internet and emerging technologies, to perpetrate crime. This study aligns with sustainable development goal (SDG) number 9 which is to "build resilient infrastructure, promote inclusive and sustainable industrialisation and foster innovation (United Nations, 2023b). Achieving

DOI: 10.4018/IJCBPL.378306

the SDGs requires cyber peace and capacity for building for the development of cyber resilience (CyberPeace Institute, 2022).

According to the South African Electronic Communication and Transaction Act of 2002, cyberfraud refers to any criminal activities perpetrated through the use of electronic communications or information systems, including any device or the internet (Republic of South Africa, 2002). The International Criminal Police Organization (INTERPOL) 2021 Africa cyberthreat assessment report indicated that South Africa tops the list of African countries that have the highest number of cybersecurity threats, with a total of 230 million threats detected (INTERPOL, 2021). The country also had the highest attempt of ransomware and business email compromise in the same year. Cyber-attacks reportedly cost the country a sum of R2.2 billion a year (INTERPOL, 2021). The increase in cybersecurity breaches in South Africa is linked to the increase in mobile banking applications and digital services which saw banking application fraud increase by 100% in 2022 (INTERPOL, 2021). Mcanyana et al. (2020) noted that South Africa has the third highest number of cybercrime victims worldwide. The use of information technology has radically transformed the way businesses and financial transactions are carried out. It has also led to the opening of more digital services to customers thereby making banking operations more accessible to customers and efficient. However, this comes with certain cyber risks, since the more financial institutions and their customers are exposed to digital services, the higher their vulnerability to cyberattack. Cyberthreat actors usually leverage the increasing reliance on digital technologies to perpetrate fraud.

Amongst other strategies that can be used to mitigate fraud risks, PwC (2020) suggested periodic conduct of risk assessment, which will enable financial institutions to effectively measure and manage risks, and compliance to regulatory and security policies as well as ethics. Furthermore, PwC (2020) proposed the adoption of a more holistic, systemic, and realistic approach towards risk management as this can promote synergy among the key anti-fraud functions. To mitigate cyber risks in the banking industry, the application of forensic accounting techniques such as evidence gathering and data analysis, surveillance, digital forensics, asset tracking, and financial statement analysis, amongst others have been proposed (Akinbowale, Klingelhöfer, et al., 2023). By employing the services of a forensic accountant, financial organisations can be more proactive in the fight against cyberfraud and promote trust in the financial operations (Akinbowale, Klingelhöfer, et al., 2023). Furthermore, the integration of forensic accounting techniques, management control systems, and big data technology have been proposed (Akinbowale et al., 2021; Akinbowale, Mashigo, et al., 2023). The implementation of management controls in the areas of access controls, transactions approvals, and authentications, oversight, quality controls, standard operating procedures and regulatory compliance, human capacity development, workflows, supervision, ethics, values, and principles can reduce the vulnerabilities of financial institutions to cyberattack. Some of the significance of big data technology in fraud mitigation include data mining, pattern recognition to identify trends linked to fraudulent activities, prevention with predictive analytics, as well as real time monitoring and anomaly detection. In addition, Akinbowale et al. (2022) suggested the adoption of the balanced scorecard that considers both financial and non-financial measures as a strategic performance management tool in the fight against cyberfraud. This is to appraise the methods employed for tackling cyberfraud and take corrective actions where necessary and to improve communication and effectively translate an organisation's strategic goal of cyberfraud mitigation into performance objectives that can be measured and monitored.

Likewise, studies suggested the deployment of digital technologies for cyberfraud mitigation, including, for instance, the use of applications and security software, real time internet banking fraud alerts tracking systems, intrusion detection systems, and so on. (Ali et al., 2017; Dzomira, 2015; Herselman & Warren, 2004). Obeng-Adjei (2017) opined that synergy among financial institutions with other stakeholders such as the government, regulators, service providers, as well as the public and private sectors on cybersecurity would yield more fruitful results. UK Finance (2020) suggested financial organisations become more proactive in their approach against cyberfraud. According to their report, the implementation of cyber threat intelligence, and cyber defence, as well as intelligence