International Journal of Cyber Behavior, Psychology and Learning
Volume 16 • Issue 1 • January-December 2026

Analysis of the Causative and Motivating Factors of Cyberfraud Perpetration in South Africa

Oluwatoyin Esther Akinbowale
http://orcid.org/0000-0001-5886-3018
Tshwane University of Technology, South Africa

Mulatu Fekadu Zerihun
http://orcid.org/0000-0003-4797-928X
Tshwane University of Technology, South Africa

Polly Mashigo
Tshwane University of Technology, South Africa
Received: June 10th, 2024 | **Accepted:** May 7th, 2026

ABSTRACT

The rate of cyberattack in South Africa continues to increase with corresponding increase in the sophistication of cyberfraud perpetration by the threat actors. This study employed the quantitative approach involving the use of a structured questionnaire as the survey instrument. Using expert sampling, key organizational staff saddled with the responsibility of cyberfraud mitigation were surveyed across the 17 licensed banks in South Africa. The factor analysis was carried out with the Statistical Package for Social Sciences, 2022 environment software, to investigate the major causative and motivating factors of the threat actors. The results obtained indicated that the three major probable causative factors of cyberfraud perpetration include installation and use of emerging technologies, weak controls by management, and poor organizational culture. Furthermore, the identified major probable motivating factors were pressure, opportunity, and greed. These factors had their eigenvalues greater than or close to 1. The study thereafter presented a framework for achieving cybersecurity and resilience.

KEYWORDS

Banking Industry, Causative and Motivating Factors, Cyberfraud, Eigenvalues, Factor Analysis

INTRODUCTION

Africa's Internet economy represents a large investment opportunity, which has a great potential to drive the African economy and development (International Finance Corporation, 2020). World Bank Report (2019) stated that South Africa is one of the digital economy leaders on the African continent and a major leader in regional digital economy development. With the growing rate of Africa's population and the Internet users, the Internet economy had the potential to increase Africa's gross domestic product (GDP) by $180 billion in U.S. dollars in 2025. This accounts for 5.2% of the total continent's GDP and, by 2050, it is projected that the Internet economy may potentially contribute $712 billion to the continent's GDP, accounting for 8.5% of the continent's total GDP. International Finance Corporation (2020) further indicated that the Internet economy was gradually transforming

DOI: 10.4018/IJCBPL.410611

the efficiency and productivity of critical industry such the economy, agriculture, education, financial services, health care, and supply chains, among others. Hence, the Internet economy plays a pivotal role in Africa's drive toward e-commerce, increasing GDP growth as well as the increasing rate of foreign investors' interests. However, the Internet also presents a potential risk for individuals, investors, businesses, and governments who are vulnerable to cyberfraud perpetration. Cassim (2016) linked the growth of cybercrime in Africa compared to other continents to the increasing number of Internet users. Interpol Report (2022) reported that South Africa had an Internet penetration rate of over 70%. The threat actors may leverage this as an opportunity to defraud unsuspecting internet users.

Surfshark (2022) reported that, in South Africa, the percentage of people who fell victim to cybercrime among a specific number of Internet users increased by 8% from 2021 to 2022. This placed South Africa in the fifth position in the global cybercrime density ranking and the first position in Africa.

The aim of this study was to analyze the causative and motivating factors of cyberfraud perpetration in South Africa with a view to providing policy recommendations for its effective mitigation. The motivation for this stemmed from the fact that South Africa was a leading player in the continental and regional Internet economy. South Africa's Internet economy could flourish more and attract more investors with effective cybersecurity. This study was significant in the sense that, since the outbreak of COVID-19, South Africa had transitioned rapidly to a hybrid work culture that combined physical and remote work environments, thereby increasing the vulnerability of cyberattack. Therefore, the study provided insights into the root causes and motivating factors of cyberfraud perpetration. When the root causes of cyberfraud perpetration were known, sustainable and innovative could be developed to combat it.

LITERATURE REVIEW

In South Africa, 56 out of a million Internet users were reported to have fallen victim of cybercrime between 2021 and 2022. This amounted to a total of 2,000 cybercrime victims. Interpol Report (2022) confirmed that South Africa was the cybercrime hub of Africa. The report of Surfshark (2022) was supported by a parallel report of Interpol Report (2022) on Africa cyberthreat assessment, which placed South Africa in the first position in the continent in the number of cybersecurity threats identified.

In 2022, a total of 230 million threats were detected, out of which 219 million were email-related threats. This implied that 95.22% of the cybercrime threats detected in South Africa in 2022 were driven by electronic mail. In Africa, South Africa also had the highest targeted ransomware and business-email-compromise threats, according to Interpol Report (2022).

Accenture (2020) reported that there were cyber vulnerabilities exploited by threat actors in South Africa, which cost the country the sum of 2.2 billion a year in South African Rand to cybercrime related incidences. According to Interpol Report (2022), South Africa witnessed a 100% increase in mobile banking application fraud with an estimate of 577 malware attacks per hour.

A report of the South African Banking Risk Information Center (SABRIC; 2019) indicated that gross fraud losses on South-African-issued cards increased by 20.5% from 2018 to 2019 due to card-not-present (CNP) fraud. CNP was a fraud category perpetrated through online transactions, in which the card of the victim was not physically presented to a merchant for a visual check before payments were made from it by the threat actors. CNP fraud, banking malware attacks, phishing, and other forms of digital fraud positioned South Africa as a leading cybercrime hub in Africa.

Another area of growing concern for South Africa is the cryptocurrency scams, in which the threat actors seek to defraud victims of their cryptocurrency. Interpol Report reported that South Africans were scammed out of $588 million and $3.6 billion in Bitcoin in 2020 and 2021, respectively. Cryptocurrency scams were becoming increasingly quite lucrative in South Africa, with the country named among the top-10 lists of countries globally where threat actors received the highest volume of cryptocurrency. In addition, threat actors also engaged in phishing, involving the use of false or