International Journal of Cyber Behavior, Psychology and Learning
Volume 14 • Issue 1 • January-December 2024

Application of Situational Crime Prevention Framework for Cybercrime Mitigation

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

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

Polly Mashigo
Tshwane University of Technology, South Africa

ABSTRACT

The purpose of this study is to apply the Situational Crime Prevention (SCP) technique to cybercrime mitigation using the South Africa cybercrime incidences as a case study. The SCP was first explained from the theoretical perspective and its five major strategies namely "increase effort", "increase risks", "reduce reward", "reduce provocation" and remove excuses" were explained and linked to remote and online crimes. Prevalent cybercrimes perpetrated in South Africa were also highlighted with hacking used specifically as an example in this study. The SCP technique was tailored towards the mitigation of hacking and its prevalent forms. The SCP fraud prevention "hardening framework" was developed and validated using the hacking incidences in South Africa as a case study. Based on this policy recommendations were made to promote cyber resilience. The outcomes of this study are conceptual frameworks with guidelines for applying the SCP strategies to remote and online crime. The conceptual frameworks are suitable for cybercrime prevention and mitigation and for achieving cyber-resilience

KEYWORDS

Cybercrime, Cybercrime Prevention and Mitigation, Cyber Resilience, Hacking, SCP

INTRODUCTION

Cybercrime, one of the fastest growing crimes across the globe, involves the use of computers and digital platforms to conduct unlawful activities driven by motives like revenge or financial gain (Toona, 2022). It is a major challenge faced by financial institutions and intent service providers, including those in South Africa.

Accenture (2020) reported that the cost incurred due to cybercrime perpetration has increased to R2.2 bn per year. The National Cybersecurity Index (2018) indicated that South Africa ranked 102 out of 160 countries in terms of cybersecurity capacity, with an estimated score of 27.27%. The Global Cybersecurity Index ranked South Africa fourth and eighth in the list of African countries vulnerable to cybersecurity breaches in 2018 and 2020, respectively (Global Cybersecurity Index, 2018, 2020). According to Cyber Exposure Index (2020), South Africa maintained the sixth position among African countries with extreme exposure to cybersecurity vulnerabilities. This report aligns

DOI: 10.4018/IJCBPL.353436

with Surfshark (2022), which revealed that South Africa ranked sixth in cybercrime density, increasing from 11.8 victims per one million internet users in 2016 to 14.1 victims in 2019 and from 50.8 victims in 2020 to 56 victims in 2021.

Researchers like Mcanyana and Brindley (2020) and Akinbowale et al. (2024a, 2024b) reported that South Africa witnessed increasing rates of cyberattacks, impacting banks, service providers, and customers. According to Toona (2022), the main targets of cybercrime in South Africa are financial institutions, insurance companies, energy and utility companies, and the government. However, any business organization can be targeted. Toona (2022) also reported that since the COVID-19 pandemic, South Africa has witnessed high profile cyberattacks on financial institutions and critical national infrastructures like the Transnet (a state-owned freight logistics organization) and South Africa's Department of Justice and Constitutional Development.

Prominent cybercrime methods include phishing, spam e-mail, denial of service (DoS), ransomware, and malware attacks. Delport (2020) reported that from January to March 2020, cyberattack cases through malware increased by 33%, while spamming attacks increased by 26.3%. The cyber defense approach employed by banks, service providers, and customers proved quite effective, with the detection of fraud via impersonation increasing by 30.3%, malware detections increasing by 35.16%, and the blocking of fraudulent links increasing by 59.8% (Delport, 2020). A survey by Akinbowale et al. (2024b) on the effectiveness of anti-fraud technologies in South African banking industries also supported the notion that South African banks deploy up-to-date technologies to effectively mitigate cybercrime.

However, the rate of cybercrime perpetration in South Africa is still on the rise. In fact, anti-fraud technologies alone cannot ensure the sustainable or effective mitigation of cybercrime perpetration. Other issues must be considered, including internal controls, synergy among stakeholders saddled with the responsibility of ensuring cybersecurity, the enactment and implementation of anti-cybercrime laws, and the development and implementation of regulatory and control frameworks. Drawbacks delaying the fight against cybercrime in South Africa include a lack of strict anti-cybercrime laws and resources for law enforcement agencies (Rick Crouch & Associates, 2020).

The efforts of the government and other stakeholders in fighting cybercrime have yielded positive results. Still, the goal of cybercrime mitigation has not been achieved holistically. It is, however, worth mentioning that the challenge of cybercrime perpetration is not limited to South Africa. This costly global problem disrupts large and small businesses and puts data and networks at risk (Deloitte, 2016).

The outbreak of COVID-19 led to a rise in the number of digital banking channels and remote banks, fueling an increase in cybercrime attacks. Cybercriminals, in turn, began to exploit the vulnerabilities of digital and remote banking systems via malicious software like viruses, worms, spyware, and Trojans. They also leverage the anonymity of cyberspace to launch attack from different locations (Deloitte, 2016). Fearn (2017) attributed the increase in cybercrime perpetration, including data breaches, to a lack of experts in cybersecurity.

In Africa, cyberthreats increase in conjunction with the growth in the number of internet users. The growing population in Africa, particularly in South Africa, is expected to contribute to more cybercrime cases unless effective and sustainable means are deployed to mitigate it (Song, 2017).

According to Rose (2020), the cost incurred by South Africa due to cybercrime-related incidences exceed ZAR 2.2 billion per year.

In 2021, the South African Banking Risk Information Centre reported that the number of cybercrime cases attributed to digital banking in South Africa decreased by 18% as compared to 2020 and those attributed to mobile banking decreased by 45% (SABRIC, 2021). However, was a 13% increase in cybercrime incidences attributed to the use of other banking applications. Comparing the cybercrime density of 2021 to 2020, Surfshark (2022) indicated that South Africa witnessed a 2% increase in cybercrime density (the percentage of cybercrime victims among a specified internet user) in 2021 as compared to 2020. Writer (2023) found that South Africa's cybercrime density increased by 8% from 2021 to 2022, placing the country in the fifth position in the global ranking of cybercrime